

# **CompTIA**

## **220-1102 Exam**

**CompTIA A+ Certification Core 2 Exam**

**Version : 24.0**  
**[Total Questions : 750]**

---

## **Question: 1**

---

A user reported that Windows has crashed several times during the day. A technician needs to check error messages to determine whether the issue pertains to the hardware or an application. Which of the following tools should the technician use?

- A. Event Viewer
- B. Resource Monitor
- C. Performance Monitor
- D. Device Manager

---

**Answer: A**

---

Explanation:

Detailed

Event Viewer (Option A) is the appropriate tool to check for system and application logs, including error messages and crash reports. It helps the technician determine the cause of the crashes by reviewing logged events.

Resource Monitor (Option B) tracks real-time usage of system resources but doesn't log errors.

Performance Monitor (Option C) monitors system performance but isn't primarily used for crash diagnostics.

Device Manager (Option D) manages hardware devices but doesn't provide crash logs.

CompTIA A+ Core 2 Reference:

3.1 - Troubleshoot common Windows OS problems using tools like Event Viewer

---

## **Question: 2**

---

A technician is helping a customer connect to a shared drive. The technician notices some unused drives that have already been mapped and wants to disconnect those drives first. Which of the following commands should the technician use?

- A . format
- B . netstat
- C . diskpart
- D . net use
- E . rmdir

---

**Answer: D**

---

Explanation:

Detailed

The net use (Option D) command is used to manage network drives in Windows. It can be used to display and disconnect mapped network drives, making it the correct choice for removing unused network drives.

format (Option A) is used to format disks, not for managing network drives.

netstat (Option B) displays network connections but doesn't manage network drives.

diskpart (Option C) is used for disk partitioning, not network drive management.

rmdir (Option E) is used to remove directories, not network drives.

CompTIA A+ Core 2 Reference:

1.2 - Use the appropriate Microsoft command-line tool, including net use for managing network drives .

---

### Question: 3

---

Which of the following languages would a technician most likely use to automate the setup of various services on multiple systems?

- A . SQL
- B . HTML
- C . PowerShell
- D . C#

---

**Answer: C**

---

Explanation:

Detailed

PowerShell (Option C) is a powerful scripting language used in Windows environments for automating tasks, including the configuration of services across multiple systems. It is widely used by system administrators for scripting and automating administrative tasks.

SQL (Option A) is used for managing databases, not for scripting system configurations.

HTML (Option B) is a markup language for web development, not for automating services.

C# (Option D) is a general-purpose programming language but is not primarily used for administrative automation tasks.

CompTIA A+ Core 2 Reference:

4.8 - Basics of scripting, including PowerShell for automation

---

### Question: 4

---

Which of the following types of malware is designed to enable administrative access to a computer?

- A . Rootkit
- B . Trojan
- C . Worm
- D . Ransomware

---

**Answer: A**

---

Explanation:

Detailed

A rootkit (Option A) is a type of malware designed to gain administrative (root) access to a system while hiding its presence. Rootkits can manipulate system processes and files to remain undetected, making them particularly dangerous.

Trojan (Option B) is malware disguised as legitimate software but doesn't necessarily provide administrative access.

Worm (Option C) spreads across networks but doesn't grant administrative access.

Ransomware (Option D) encrypts data and demands a ransom but doesn't typically provide ongoing administrative access.

CompTIA A+ Core 2 Reference:

2.3 - Explain malware types, including rootkits and their purpose .

---

### **Question: 5**

---

Internet speeds on a user's Windows 10 device are slow, but other devices on the same network are running at normal speeds. A technician thinks the issue may be related to the proxy settings. Which of the following should the technician check to verify the proxy configuration?

- A . Network and Sharing Center
- B . Internet Options
- C . Firewall settings
- D . System settings

---

**Answer: B**

---

Explanation:

Detailed

The correct place to check proxy settings in Windows 10 is under Internet Options (Option B), specifically in the 'Connections' tab. Proxy configurations can affect internet speeds if misconfigured or if a proxy is being used unnecessarily.

Network and Sharing Center (Option A) provides information on network connections but doesn't handle proxy settings.

Firewall settings (Option C) manage network traffic rules but don't directly affect proxy settings.

System settings (Option D) contain general system configurations, not specific to proxy settings.

CompTIA A+ Core 2 Reference:

1.6 - Configure networking features in Windows, including proxy settings

---

### **Question: 6**

---

Which of the following ensures proprietary information on a lost or stolen mobile device cannot be accessed while the device is offline?

- A . Remote wipe
- B . Mandatory screen locks
- C . Location applications
- D . Device data encryption

---

**Answer: D**

---

Explanation:

Detailed

Device data encryption (Option D) ensures that even if the device is lost or stolen, its data cannot be accessed without proper credentials, even while offline. Encryption protects the data at rest, making it unreadable without the decryption key.

Remote wipe (Option A) requires the device to be online to receive the wipe command.

Mandatory screen locks (Option B) provide a layer of security but can be bypassed with physical access in some cases.

Location applications (Option C) help track the device but don't protect data.

CompTIA A+ Core 2 Reference:

2.7 - Explain methods for securing mobile devices, including encryption

---

### **Question: 7**

---

A user's corporate iPhone had issues and was repaired while the user was on vacation. The mobile phone has been compared to an identical phone. Which of the following best describes what is happening to the phone?

- A . APK Source

- B . Connectivity issues
- C . Developer Mode
- D . Jailbreak

---

**Answer: D**

---

Explanation:

Detailed

A jailbroken iPhone (Option D) allows users to bypass Apple's restrictions to install unauthorized apps and modify system settings. This situation suggests the phone may have been compromised or tampered with, potentially voiding warranties and exposing the device to security vulnerabilities.

APK Source (Option A) refers to Android packages, not applicable to iPhones.

Connectivity issues (Option B) doesn't explain the comparison to an identical phone.

Developer Mode (Option C) is typically used for app development, not indicative of the situation.

CompTIA A+ Core 2 Reference:

2.7 - Explain mobile device security, including risks of jailbreaking

---

### **Question: 8**

---

A technician is setting up a wireless network in a small, crowded office and wants to minimize Wi-Fi access. Which of the following security settings should the technician enable?

- A . Port forwarding
- B . Unused ports
- C . SSID broadcast
- D . Allow list

---

**Answer: D**

---

Explanation:

Detailed

Enabling an allow list (Option D) will limit access to the wireless network by only allowing devices with specified MAC addresses to connect. This is an effective method for minimizing Wi-Fi access in a crowded environment.

Port forwarding (Option A) controls traffic through specific ports but doesn't minimize wireless access.

Unused ports (Option B) could refer to physical network ports or firewall settings, unrelated to controlling Wi-Fi access.

Disabling SSID broadcast (Option C) might hide the network name but doesn't secure access.

CompTIA A+ Core 2 Reference:

2.9 - Configure security settings for SOHO networks, including MAC filtering .

---

### Question: 9

---

A technician thinks that a computer on the network has been infected with malware. The technician attempts several times to use a malware removal tool, but the issue persists. Which of the following should the technician do next?

- A . Restore the computer from the last known-good backup
- B . Reboot the computer into safe mode
- C . Purchase a new endpoint protection tool
- D . Use system recovery to prevent further infection

---

**Answer: B**

---

Explanation:

Detailed

Rebooting the computer into safe mode (Option B) limits the processes and services that run, which can help in isolating and removing persistent malware that might be hiding in normal mode. Safe mode provides a cleaner environment to troubleshoot and remove malware.

Restoring from a backup (Option A) may work but should be considered after attempts to clean the infection.

Purchasing a new endpoint protection tool (Option C) is unnecessary at this stage since existing tools can be run in safe mode.

Using system recovery (Option D) could potentially remove the infection, but it's a more drastic step that may not be necessary yet.

CompTIA A+ Core 2 Reference:

3.3 - Best practices for malware removal, including booting into safe mode

---

### Question: 10

---

A customer reports that an Android phone will not allow the use of contactless electronic payment. Which of the following needs to be enabled to resolve the issue?

- A . Wi-Fi
- B . Nearby share
- C . NFC
- D . Bluetooth

---

**Answer: C**

---

Explanation:

Detailed

To enable contactless payment, NFC (Near Field Communication) (Option C) needs to be enabled. NFC is the technology used in most mobile payment systems to enable close-range communication between the phone and a payment terminal.

Wi-Fi (Option A) and Bluetooth (Option D) are unrelated to contactless payments.

Nearby share (Option B) is a file-sharing feature, not a payment technology.

CompTIA A+ Core 2 Reference:

2.7 - Explain common mobile device security settings, including enabling NFC for mobile payments.

---

**Question: 11**

---

Due to special job responsibilities, an end user needs the ability to edit the properties of Windows system files. The user has already been granted local administrator privileges. Which of the following Control Panel utilities should be used to provide easy access to the files?

- A . File Explorer Options
- B . Ease of Access
- C . Indexing Options
- D . Administrative Tools

---

**Answer: D**

---

Explanation:

Detailed

The correct answer is Administrative Tools (Option D), which provides access to several system utilities, including those needed for managing system files and settings. Since the user already has local administrator privileges, this would allow them to edit system properties efficiently.

File Explorer Options (Option A) manage general file display settings but do not provide administrative access.

Ease of Access (Option B) is related to accessibility settings, not file management.

Indexing Options (Option C) control how files are indexed for search, but are unrelated to system file editing.

CompTIA A+ Core 2 Reference:

1.3 - Use features and tools of the Windows operating system, including Administrative Tools.

---

## **Question: 12**

---

A technician needs to implement password requirements that apply to all domain-joined computers. Which of the following commands should the technician most likely run?

- A . gpupdate
- B . devmgmt
- C . regedit
- D . resmon

---

**Answer: A**

---

Explanation:

Detailed

The correct command is gpupdate (Option A), which refreshes Group Policy settings. To implement password requirements across domain-joined computers, the policy would be set via Group Policy, and then running the gpupdate command ensures that the new settings are applied to all systems.

devmgmt (Option B) opens Device Manager, which is unrelated to Group Policy.

regedit (Option C) opens the Windows Registry Editor, which is not used for group-wide password policy settings.

resmon (Option D) opens Resource Monitor, which helps monitor system resources, not Group Policy.

CompTIA A+ Core 2 Reference:

1.5 - Using appropriate Windows settings, including password policies via Group Policy.

---

## **Question: 13**

---

A user's PC is performing slowly after the user clicked on a suspicious email attachment. The technician notices that a single process is taking 100% of RAM, CPU, and network resources. Which of the following should the technician do first?

- A . Disconnect the computer from the network
- B . Run an antivirus scan
- C . Reboot the computer
- D . Educate the user about cybersecurity best practices

---

**Answer: A**

---

Explanation:

Detailed

The technician should disconnect the computer from the network (Option A) first to prevent any further spread of the infection or data loss. Once the machine is isolated from the network, the technician can safely investigate the malware without risking infection to other systems.

Running an antivirus scan (Option B) comes after isolating the system.

Rebooting the computer (Option C) could lead to the loss of critical information or make it harder to diagnose the issue.

Educating the user (Option D) is important but should happen after resolving the immediate issue.

CompTIA A+ Core 2 Reference:

3.3 - Best practices for malware removal, including isolating the system first.

---

### **Question: 14**

---

A technician is deploying a new Wi-Fi solution for the office and wants to ensure users can log in to the Wi-Fi with their existing network log-in and password. Which of the following methods should the technician use?

- A . AES
- B . RADIUS
- C . TKIP
- D . WPA3

---

**Answer: B**

---

Explanation:

Detailed

RADIUS (Remote Authentication Dial-In User Service) (Option B) is a network protocol that allows users to authenticate using their network credentials, such as usernames and passwords, typically stored in a central directory like Active Directory. It ensures that users can log in to the Wi-Fi using their existing network credentials.

AES (Option A) is an encryption standard but does not handle authentication.

TKIP (Option C) is a deprecated encryption protocol and not related to network login management.

WPA3 (Option D) is the latest Wi-Fi security standard but does not specifically handle centralized login management like RADIUS does.

CompTIA A+ Core 2 Reference:

2.2 - Compare and contrast wireless security protocols and authentication methods, including RADIUS.

---

### **Question: 15**

---

The following error is displayed on a user's computer screen:

No operating system found

Which of the following is the first troubleshooting step a technician should complete?

- A . Disconnect external storage
- B . Flash the BIOS
- C . Replace the SATA cable
- D . Turn on the device in safe mode

---

**Answer: A**

---

Explanation:

Detailed

The first step is to disconnect external storage (Option A). Sometimes, the system may be attempting to boot from an external drive or USB device instead of the internal hard drive. By removing the external storage, the system will attempt to boot from the correct drive.

Flashing the BIOS (Option B) is more complex and typically unnecessary for this issue.

Replacing the SATA cable (Option C) may help if there's a hardware issue, but it's not the first troubleshooting step.

Turning on the device in safe mode (Option D) would not work if no operating system is detected.

CompTIA A+ Core 2 Reference:

5.1 - Apply troubleshooting methodologies, including steps for resolving boot issues.

---

### **Question: 16**

---

A technician is reusing several hard drives to increase local storage on company workstations. The drives contain PII that is no longer needed. Which of the following should the technician do to prevent unauthorized access to the data?

- A . Degauss the drives
- B . Drill through the drives
- C . Wipe the drives
- D . Reimage the drives

---

**Answer: C**

---

Explanation:

Detailed

The appropriate method to prevent unauthorized access to sensitive data is to wipe the drives (Option C). Wiping ensures that all data is securely erased, preventing any possibility of recovery. This is essential when handling drives containing Personally Identifiable Information (PII).

Degaussing (Option A) erases data but is more commonly used for magnetic tapes.

Drilling through the drives (Option B) physically destroys the drives, which may not be necessary if they are being reused.

Reimaging (Option D) would overwrite the current data with new data but may not guarantee complete data destruction.

CompTIA A+ Core 2 Reference:

2.8 - Use common data destruction and disposal methods, including securely wiping drives.

---

### **Question: 17**

---

Which of the following applications allows a user to create backups in macOS?

- A . Time Machine
- B . FileVault
- C . Keychain
- D . Mission Control

---

**Answer: A**

---

Explanation:

Detailed

Time Machine (Option A) is macOS's built-in backup application. It allows users to automatically back up their entire system, including apps, music, photos, emails, and system files. Time Machine provides an easy way to restore files from a previous state or recover from a system failure.

FileVault (Option B) is used for encrypting data, not for backups.

Keychain (Option C) is a password management tool.

Mission Control (Option D) manages open windows and desktops but has no backup functionality.

CompTIA A+ Core 2 Reference:

1.10 - Features and tools of macOS, including backup options like Time Machine.

---

### **Question: 18**

---

A user's mobile phone battery does not last long and navigation is very slow. Which of the following should the technician do first to resolve the issue?

- A . Uninstall unused programs
- B . Check running applications
- C . Update the mobile OS
- D . Disable network services

---

**Answer: B**

---

Explanation:

Detailed

The first step is to check running applications (Option B). Applications running in the background could consume a lot of battery and processing power, causing slow performance and battery drain. By identifying and closing or uninstalling these apps, the technician can resolve the issue more effectively.

Uninstalling unused programs (Option A) might help, but checking active applications is more immediate.

Updating the mobile OS (Option C) can improve performance but is not the first step in this scenario.

Disabling network services (Option D) might help reduce battery drain but does not address potential app-related issues.

CompTIA A+ Core 2 Reference:

3.4 - Troubleshoot common mobile OS and application issues, including battery and performance concerns.

---

### **Question: 19**

---

A technician received a notification about encrypted production data files and thinks active ransomware is on the network. The technician isolated and removed the suspicious system from the network. Which of the following steps should the technician take next?

- A . Schedule and perform an antivirus scan and system update
- B . Educate the end user on internet usage
- C . Perform a system scan to remove the malware
- D . Create a system restore point

---

**Answer: C**

---

Explanation:

Detailed

The next step after isolating the system is to perform a system scan to remove the malware (Option C). Since ransomware is suspected, running a comprehensive malware scan can help identify and remove the malicious software. It is crucial to deal with the active threat before taking further actions.

Scheduling an antivirus scan and system update (Option A) may help, but the immediate concern is identifying and removing the ransomware.

Educating the end user (Option B) is important but should happen after the immediate threat is resolved.

Creating a system restore point (Option D) would not be useful at this point since the system is infected.

CompTIA A+ Core 2 Reference:

2.3 - Detect, remove, and prevent malware, including handling ransomware.

---

### **Question: 20**

---

Which of the following is protected by government policy for end-user information?

- A . DRM
- B . EULA
- C . PCI
- D . PII

---

**Answer: D**

---

Explanation:

Detailed

Personally Identifiable Information (PII) (Option D) is protected by government regulations. PII includes sensitive data such as names, addresses, social security numbers, and other information that can identify individuals. Various laws, such as GDPR and HIPAA, mandate the protection of PII.

DRM (Option A) refers to digital rights management, which controls access to digital media.

EULA (Option B) refers to software licensing agreements.

PCI (Option C) relates to payment card industry standards for handling cardholder information but is more specific to payment data than general PII.

CompTIA A+ Core 2 Reference:

4.6 - Explain prohibited content and privacy concepts, including the protection of PII.

---

### **Question: 21**

---

Which of the following attacks can a hacker use to execute code on a user's computer when the user visits a specially prepared, malicious website?

- A . DoS
- B . Spoofing

- C . XSS
- D . SQL injection

---

**Answer: C**

---

Explanation:

Detailed

Cross-site scripting (XSS) (Option C) allows attackers to inject malicious scripts into web pages viewed by users. When the user visits the compromised site, the script runs in the user's browser, potentially allowing the attacker to steal data or perform unauthorized actions. XSS is a common vulnerability in web applications that allows code execution.

DoS (Option A) disrupts services but doesn't involve executing code on a user's device.

Spoofing (Option B) involves impersonating another device or user but doesn't execute code.

SQL injection (Option D) attacks a database and is unrelated to executing code on the user's computer.

CompTIA A+ Core 2 Reference:

2.4 - Explain common social engineering attacks, including XSS.

---

## **Question: 22**

---

A developer installed a new software package that has stopped all file server access. Which of the following change management practices should have been followed?

- A . End-user acceptance
- B . Staff delegation
- C . Appropriate scoping
- D . Sandbox testing

---

**Answer: D**

---

Explanation:

Detailed

The issue could have been avoided if the developer had used Sandbox testing (Option D), which allows new software to be tested in a controlled environment before implementation. This process ensures that the software does not negatively impact system functionality, like stopping access to critical resources such as file servers.

End-user acceptance (Option A) ensures that users approve the software, but it wouldn't prevent the issue.

Staff delegation (Option B) relates to who is responsible but doesn't address testing.

Appropriate scoping (Option C) helps in defining the extent of changes but does not replace testing.

CompTIA A+ Core 2 Reference:

4.2 - Explain basic change management best practices, including testing in a sandbox environment.

---

### Question: 23

---

A customer reports high data usage on a smartphone that reaches its monthly data limit within the first week of each billing cycle. The customer uses the phone primarily for calls and SMS messages with minimal content streaming. A technician troubleshoots the phone and notices that both developer mode and installs from unknown sources are enabled. Which of the following should the technician check next?

- A . Storage cache
- B . Malicious applications
- C . Privacy settings
- D . Permissions

---

**Answer: B**

---

Explanation:

Detailed

Since both developer mode and the ability to install apps from unknown sources are enabled, the technician should check for Malicious applications (Option B). Unknown sources can allow unverified apps that may include malware or apps that use excessive background data without the user's knowledge. Checking for malicious apps is essential in this scenario.

Storage cache (Option A) would not typically cause high data usage.

Privacy settings (Option C) control data sharing and permissions but don't directly impact data usage.

Permissions (Option D) might help identify apps using data, but the focus should be on apps that could be malicious.

CompTIA A+ Core 2 Reference:

2.7 - Explain common methods for securing mobile devices, including detecting and preventing malware.

---

### Question: 24

---

A technician is installing an operating system on a new computer. Which of the following is the first step of the process?

- A . Setting the boot order
- B . Formatting the hard drive
- C . Entering the product key
- D . Selecting the filesystem

---

**Answer: A**

---

Explanation:

Detailed

The first step in installing an operating system on a new computer is Setting the boot order (Option A). This ensures that the computer can boot from the installation media (USB, DVD, etc.). Once the boot order is configured, the system can start from the installation source, and the rest of the OS installation process can proceed.

Formatting the hard drive (Option B) comes later in the process, after the installation media is booted.

Entering the product key (Option C) and Selecting the filesystem (Option D) are subsequent steps during the installation process.

CompTIA A+ Core 2 Reference:

1.9 - Perform OS installations and upgrades, including setting boot methods and boot order.

---

**Question: 25**

---

A technician is creating a Windows splash screen that details login expectations. Which of the following should the technician most likely use?

- A . End-user license agreement
- B . Non-disclosure agreement
- C . Regulatory compliance
- D . Acceptable use policy

---

**Answer: D**

---

Explanation:

Detailed

The appropriate choice is 'Acceptable Use Policy' (Option D). This policy defines the rules for how users should use the system, including login expectations and proper behavior when using company resources. It's typically displayed as a splash screen to remind users of their responsibilities.

End-user license agreement (Option A) pertains to the terms of software usage.

Non-disclosure agreement (Option B) deals with confidentiality but is unrelated to login behavior.

Regulatory compliance (Option C) relates to adherence to laws and regulations, but it is not typically displayed on a splash screen for login expectations.

CompTIA A+ Core 2 Reference:

4.6 - Explain the importance of prohibited content/activity and acceptable use policies.

---

### Question: 26

---

A technician is configuring a workstation's security settings, and the following options are available:

Account lockout policy

Group policy

Two-factor authentication

Password complexity requirements

Firewalls

User accounts

Access control lists

Antivirus software

Which of the following settings should the technician configure to deploy strong password enforcement across the enterprise?

A . Account lockout policy

B . Group policy

C . Two-factor authentication

D . Access control lists

---

### Answer: B

---

Explanation:

Detailed

The technician should configure 'Group Policy' (Option B) to enforce password complexity across the enterprise. Group Policy in a Windows environment allows administrators to manage various settings, including password policies, at a domain level. This can include enforcing complexity requirements (such as minimum length, use of uppercase, lowercase, and special characters), expiration times, and other security measures.

Account lockout policy (Option A) controls how many failed login attempts trigger a lockout but does not handle password complexity.

Two-factor authentication (Option C) is an additional security measure requiring a second form of authentication, but it does not enforce password policies.

Access control lists (Option D) define which users or systems have access to resources, not how passwords are managed.

CompTIA A+ Core 2 Reference:

2.6 - Configure workstation security best practices, including password complexity and group policies.

---

### Question: 27

---

Which of the following is used to detect and record access to restricted areas?

- A . Bollards
- B . Video surveillance
- C . Badge readers
- D . Fence

---

**Answer: C**

---

Explanation:

Badge readers are devices that scan employee or visitor credentials, logging entries and exits from restricted areas. Video surveillance (B) provides a visual record but does not directly control access. Bollards (A) and fences (D) provide physical security but cannot detect or record access events.

---

### Question: 28

---

A technician is troubleshooting a PC that will not run Windows Defender. Windows Defender has been disabled, and no other antivirus is installed on the PC. Which of the following would have caused this issue?

- A . Ransomware
- B . Rootkit
- C . Spyware
- D . Keylogger

---

**Answer: B**

---

Explanation:

Rootkits are particularly dangerous because they modify the operating system to hide their presence and can disable antivirus software like Windows Defender. Ransomware (A) encrypts files, but usually does not disable antivirus software. Spyware (C) and Keyloggers (D) typically do not directly disable antivirus programs either.

---

### Question: 29

---

A technician has been tasked with installing a workstation that will be used for point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?

- A . Data-in-transit encryption
- B . File encryption
- C . USB drive encryption
- D . Disk encryption

---

**Answer: D**

---

Explanation:

Disk encryption is the best method for securing a workstation used in financial transactions, such as point-of-sale systems. It ensures that if the workstation is stolen, all data on the disk is encrypted and cannot be accessed without proper credentials. File encryption (B) only encrypts individual files, and USB drive encryption (C) only applies to removable storage. Data-in-transit encryption (A) is not relevant for physical security.

---

### **Question: 30**

---

After a failed attempt to open an email attachment for an unexpected overdue invoice, a smartphone user experiences abnormal performance when using their mobile browser and other applications. The user restarts the device, but the issue persists. Which of the following actions should the user take next?

- A . Shut down and cold start the smartphone
- B . Delete the email containing the attachment
- C . Wipe the device and reset it to factory defaults
- D . Uninstall and reinstall the mobile browser

---

**Answer: C**

---

Explanation:

In this case, abnormal behavior after opening a suspicious email suggests malware might have infected the device. A full factory reset is recommended to remove any persistent malware, especially when a restart does not resolve the issue. Deleting the email or reinstalling the browser will not remove the malware already on the device.

---

### **Question: 31**

---

A technician is trying to perform an in-place upgrade of a Windows OS from a file. When the technician double-clicks the file, the technician receives a prompt to mount a drive. Which of the following file types did the technician download?

- A . msi
- B . iso
- C . zip
- D . exe

---

**Answer: B**

---

Explanation:

The file type ISO is a disk image format that contains everything from a CD, DVD, or Blu-ray disc in a single file. When an ISO file is accessed, the system prompts the user to mount it as a virtual drive, which is why the technician received a 'mount a drive' prompt. MSI (A) is for installing software, ZIP (C) is a compressed file, and EXE (D) is an executable file.

---

### **Question: 32**

---

Which of the following best describes XFS?

- A . A filesystem used by the Linux OS
- B . A filesystem used by iOS
- C . A filesystem used by the Windows OS
- D . A filesystem used by macOS

---

**Answer: A**

---

Explanation:

XFS is a high-performance filesystem created by Silicon Graphics in 1994 and is commonly used by Linux operating systems. It supports large files and directories and is known for its robustness and scalability. Other filesystems like NTFS (Windows), APFS (macOS), and HFS (macOS) are used on different platforms.

---

### **Question: 33**

---

Which of the following is the most practical method to reduce the number of clicks on phishing emails for a public-facing organization?

- A . Providing user awareness education
- B . Introducing a BYOD policy
- C . Setting up SMTP filtering rules
- D . Restricting emails from personal email addresses

---

**Answer: A**

---

Explanation:

User awareness education is the most effective method for reducing phishing attacks. Training users to recognize suspicious emails, links, and attachments can prevent them from falling for phishing attempts. Technical solutions like

SMTP filtering (C) and restricting emails (D) can help but are not as effective without user vigilance. A BYOD policy (B) does not directly address phishing email threats.

---

### Question: 34

---

A technician needs to disable guest log-ins on domain-joined desktop machines. Which of the following should the technician use?

- A . Group Policy
- B . Firewall
- C . Microsoft Management Control
- D . MSConfig

---

**Answer: A**

---

Explanation:

Disabling guest accounts on domain-joined machines is done through Group Policy. Group Policy allows centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. By using the Group Policy Editor (gpedit.msc), administrators can enforce policies such as disabling the guest account across all machines within the domain. The other options (Firewall, Microsoft Management Console, MSConfig) do not provide functionality specific to managing user accounts in this context.

---

### Question: 35

---

Which of the following is a preventive physical security control?

- A . Video surveillance system
- B . Bollards
- C . Alarm system
- D . Motion sensors

---

**Answer: B**

---

Explanation:

Detailed Explanation with Core 2 Reference:

Bollards are physical barriers that prevent unauthorized vehicle access to certain areas, providing a preventive measure against unauthorized entry and potential threats. Bollards are classified as a preventive control because they act to deter or block physical access to secured locations, as opposed to video surveillance or alarm systems, which are typically used for detection and monitoring. Core 2 highlights the importance of implementing various physical security controls to protect assets and infrastructure (Core 2 Objective 2.1).

---

### **Question: 36**

---

A user reports some single sign-on errors to a help desk technician. Currently, the user is able to sign in to the company's application portal but cannot access a specific SaaS-based tool. Which of the following would the technician most likely suggest as a next step?

- A . Reenroll the user's mobile device to be used as an MFA token.
- B . Use a private browsing window to avoid local session conflicts.
- C . Bypass single sign-on by directly authenticating to the application.
- D . Reset the device being used to factory defaults.

---

**Answer: B**

---

Explanation:

Detailed Explanation with Core 2 Reference:

Using a private browsing window can help resolve session conflicts by not relying on cached credentials, which might interfere with single sign-on processes. Core 2 objectives include troubleshooting authentication issues and resolving potential conflicts with single sign-on systems (Core 2 Objective 4.7).

---

### **Question: 37**

---

A technician is troubleshooting a PC that will not run Windows Defender. Windows Defender has been disabled and no other antivirus is installed on the PC. Which of the following would have caused this issue?

- A . Ransomware
- B . Rootkit
- C . Spyware
- D . Keylogger

---

**Answer: B**

---

Explanation:

Detailed Explanation with Core 2 Reference:

Rootkits can disable antivirus programs, including Windows Defender, as they operate at a low level within the OS to avoid detection. This issue falls under malware types and removal strategies in Core 2 (Core 2 Objective 2.3).

---

### **Question: 38**

---

A systems administrator at a small company wants to discretely access user machines and verify patch levels without users noticing. Which of the following remote access technologies should the administrator use?

- A . RDP
- B . MSRA
- C . SSH
- D . VNC

---

**Answer: C**

---

Explanation:

Detailed Explanation with Core 2 Reference:

SSH allows for remote access to systems securely and discretely, suitable for verifying patch levels and other administrative tasks. This meets Core 2 objectives on using secure remote access tools (Core 2 Objective 4.9).

---

### **Question: 39**

---

A user is unable to access the company's network. A technician learns the user's account became inaccessible after multiple unsuccessful login attempts. The user also changed their password before the issue started. Which of the following steps should the technician take to resolve the issue?

- A . Escalate the user's issue to the network team.
- B . Reset the user's password.
- C . Unlock the user's account.
- D . Verify the user's login and password.

---

**Answer: C**

---

Explanation:

Detailed Explanation with Core 2 Reference:

If multiple unsuccessful attempts led to the account being locked, the technician should unlock the account. Core 2 covers user account management practices, including unlocking accounts and managing failed login attempts (Core 2 Objective 2.5).

---

### **Question: 40**

---

A company is transitioning to a new firewall and discovers that one of the servers is still sending traffic to the old firewall. Which of the following IP address settings should a technician change to resolve this issue?

- A . Dynamic
- B . Gateway
- C . NAT
- D . DNS server

---

**Answer: B**

---

Explanation:

Detailed Explanation with Core 2 Reference:

The default gateway directs network traffic to external networks. If the traffic is still going to the old firewall, updating the gateway setting will redirect it to the new firewall. This task is part of network configuration management covered in Core 2 (Core 2 Objective 2.5).

---

**Question: 41**

---

A user asks a technician for recommendations to back up desktop data from a Windows OS. The technician recommends implementing daily full backups, but the user is concerned about having enough space. Which of the following additional backup methods should the technician recommend?

- A . Transaction log
- B . Incremental
- C . Synthetic
- D . Differential

---

**Answer: B**

---

Explanation:

Detailed Explanation with Core 2 Reference:

Incremental backups only save changes made since the last backup, significantly reducing storage space requirements compared to full backups. This approach is consistent with the Core 2 objective of understanding various backup methods and their space requirements (Core 2 Objective 4.3).

---

**Question: 42**

---

A user is unable to open personal files on a PC on a home network. An on-screen message indicates the files are encrypted and demands payment to access the files. Which of the following should a technician recommend the user do first?

- A . Reinstall the OS.
- B . Run the System Restore feature.
- C . Disconnect the PC from the network.
- D . Pay the amount demanded.
- E . Scan the PC with an anti-malware program.

---

**Answer: C**

---

Explanation:

Detailed Explanation with Core 2 Reference:

The PC is likely infected with ransomware. The immediate step should be to disconnect from the network to prevent the malware from spreading to other devices. Core 2 highlights steps to respond to malware incidents, such as disconnecting from the network as part of containment measures (Core 2 Objective 2.3).

---

### **Question: 43**

---

Which of the following languages would a technician most likely use to automate the setup of various services on multiple systems?

- A . SQL
- B . HTML
- C . PowerShell
- D . C#

---

**Answer: C**

---

Explanation:

Detailed Explanation with Core 2 Reference:

PowerShell is a powerful scripting language used in Windows environments to automate administrative tasks and configure services across multiple systems. According to Core 2, understanding scripting languages like PowerShell is essential for automating administrative functions (Core 2 Objective 4.8).

---

### **Question: 44**

---

A technician is replacing the rack mount UPS. Which of the following should the technician consider?

- A . Determining the availability of compressed air
- B . Getting assistance to lift the hardware
- C . Checking local low-voltage regulations
- D . Testing the fire suppression system

---

**Answer: B**

---

Explanation:

Detailed Explanation with Core 2 Reference:

Rack-mounted UPS units are often heavy, so technicians should seek assistance to lift them to avoid injury, following safety procedures. Core 2 includes handling hardware safely as part of best practices (Core 2 Objective 4.4).

---

### Question: 45

---

A technician discovers a user's PC has a 'No OS found' error message. Which of the following steps should the technician take next?

- A . Remove external storage and reboot the PC.
- B . Replace the SSD and run disk defragmenter.
- C . Start up in safe mode and roll back the latest security updates.
- D . Back up personal data and rebuild the user profile.

---

**Answer: A**

---

Explanation:

Detailed Explanation with Core 2 Reference:

A 'No OS found' message often occurs if the PC is trying to boot from an external storage device that does not contain an OS. Removing any external devices and rebooting can resolve this issue. This approach is part of troubleshooting boot-related problems, as emphasized in Core 2 (Core 2 Objective 3.1).

---

### Question: 46

---

A proxy server is required for internet access from a corporate network. Which of the following should a technician perform to manually configure a Windows 10 device for internet access?

- A . Add the proxy server's URL and IP address to the computer's hosts file under C:\windows\System32\drivers\etc.
- B . Enable the use of a proxy server and enter an address for it under Control Panel > Internet Options > Connections > LAN settings.
- C . Open a command prompt and run ipconfig /release, followed by ipconfig /renew.
- D . Set the proxy server as the default gateway under the computer's network connection IP settings by selecting Manual, then entering the proxy server's IP address under Gateway.

---

**Answer: B**

---

Explanation:

Detailed Explanation with Core 2 Reference:

Configuring a proxy server in Windows 10 can be done through the Internet Options under LAN settings, where the user can enable and enter a proxy server's address. This aligns with Core 2's objectives of configuring network

settings in a Windows environment (Core 2 Objective 1.4).

---

### Question: 47

---

A technician runs a command and gets the following output:

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . : reddog.microsoft.com

Link-local IPv6 Address ..... : fe80::de3d:9283:4f00:856a%5

IPv4 Address.....: 10.203.10.16

Subnet Mask ..... : 255.255.255.0

Default Gateway ..... : 10.203.10.1

Which of the following commands did the technician use?

- A . ipconfig
- B . tracert
- C . whoami
- D . net use

---

**Answer: A**

---

Explanation:

Detailed Explanation with Core 2 Reference:

The ipconfig command displays the IP address, subnet mask, and default gateway for all network adapters in a Windows computer. This output specifically shows details about an Ethernet adapter, which is directly tied to ipconfig. According to Core 2, understanding command-line tools like ipconfig is essential for network troubleshooting (Core 2 Objective 1.2).

---

### Question: 48

---

Several computers have been infected with malware, causing the company network to slow down and sensitive company information to be lost. The IT department installs new antivirus software to remove the malware and needs to decide the best method to prevent future malware infections. Which of the following methods would be the most effective?

- A . Encrypting data at rest
- B . Implementing firewalls
- C . Utilizing Intrusion detection systems
- D . Backing up data regularly

Explanation:

Detailed Explanation with Core 2 Reference:

Intrusion Detection Systems (IDS) monitor network traffic for malicious activities and alert administrators, helping to prevent malware infections before they can impact the network significantly. CompTIA Core 2 emphasizes the importance of implementing preventive measures like IDS to proactively detect and respond to potential threats (Core 2 Objective 2.3).

---

**Question: 49**

---

A security administrator teaches all of an organization's staff members to use BitLocker To Go. Which of the following best describes the reason for this training?

- A . To ensure that all removable media is password protected in case of loss or theft
- B . To enable Secure Boot and a BIOS-level password to prevent configuration changes
- C . To enforce VPN connectivity to be encrypted by hardware modules
- D . To configure all laptops to use the TPM as an encryption factor for hard drives

Explanation:

Detailed Explanation with Core 2 Reference:

BitLocker To Go is a feature in Windows that allows for encryption of removable drives to protect sensitive information. Training staff on BitLocker To Go ensures that if a removable drive is lost or stolen, it will be password-protected and encrypted, making the data inaccessible to unauthorized individuals. This aligns with Core 2 objectives related to security measures for data-at-rest encryption and best practices for safeguarding information (CompTIA A+ Core 2 Objective 2.6).

---

**Question: 50**

---

A technician is updating the OS on a number of Windows workstations. After successfully updating several workstations, the technician receives an error indicating that the upgrade takes more space than is available on one of the PCs. Which of the following should the technician do to proceed with the upgrade? (Select two).

- A . Unplug the extra hardware.
- B . Delete unnecessary files.
- C . Update the driver software.
- D . Restore the system files.
- E . Uninstall unused desktop applications.

F . Add additional memory.

---

**Answer: B, E**

---

Explanation:

To free up space for the upgrade, the technician should delete unnecessary files and uninstall unused desktop applications. These actions will clear storage, making room for the update. Additional memory would not solve a storage issue, and driver updates are not relevant to the storage space problem.

---

### **Question: 51**

---

A technician is trying to perform an in-place upgrade of a Windows OS from a file. When the technician double-clicks the file, the technician receives a prompt to mount a drive. Which of the following file types did the technician download?

- A .msi
- B .iso
- C .zip
- D .exe

---

**Answer: B**

---

Explanation:

An .iso file is a disk image file that needs to be mounted or burned to a physical or virtual drive. When the technician is prompted to mount the drive, it indicates that the file is an ISO, and they must mount it to proceed with the installation.

---

### **Question: 52**

---

A user downloads an application with a plug-in that is designed to automatically prompt for an OTP when the user browses to a specific website. The plug-in installs without any warnings or errors. The first time the user goes to the site, the prompt does not open, and the user cannot access the site. Which of the following browser settings should the user configure?

- A . Extensions/add-ins
- B . Certificate validity
- C . Proxy settings
- D . Trusted sources

---

**Answer: A**

---

Explanation:

The user should configure extensions/add-ins. Since the issue involves a browser plug-in, checking if the extension or add-in is enabled or properly configured can resolve the issue. If the plug-in is disabled, the OTP prompt will not appear as expected.

---

### **Question: 53**

---

Which of the following methods is a way to superficially delete files on a hard drive?

- A . Drilling
- B . Degaussing
- C . Wiping
- D . Shredding
- E . Low-level formatting

---

**Answer: A**

---

Explanation:

Drilling is a method of physically damaging the hard drive by drilling holes through it, which renders the drive inoperable. However, it is not a secure method for ensuring data cannot be recovered. Methods such as wiping or degaussing are more secure.

---

### **Question: 54**

---

A change management review board denied an administrator's request for change. The administrator had provided the purpose and scope of the change, the date and time, and impacted systems with the risk analysis. Which of the following should be included to approve this change?

- A . End-user acceptance
- B . Cost analysis
- C . Rollback plan
- D . Standard maintenance window

---

**Answer: C**

---

Explanation:

A rollback plan is essential for a change to be approved by a change management review board. It outlines the steps to reverse a change in case something goes wrong, minimizing downtime and mitigating risk. Other items like end-user acceptance and cost analysis are important but not typically the deciding factor for approval.

---

### **Question: 55**

---

A computer is restarting automatically and displaying the following error message: 'Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete).' Which of the following should the technician do first to diagnose the issue?

- A . Check the system event logs.
- B . Verify the hardware driver versions.
- C . Install Windows updates.
- D . Perform a RAM diagnostic.

---

**Answer: A**

---

Explanation:

The first step is to check the system event logs using tools like Event Viewer. This will allow the technician to identify any critical errors or warnings that occurred before the restart. Based on these logs, further troubleshooting can be done. Verifying driver versions and performing diagnostics can follow once the root cause is identified.

---

### **Question: 56**

---

A user calls the help desk to report an issue with their smartphone. After the user returns from a business trip, the user is no longer able to access email or visit websites without a Wi-Fi connection on the smartphone. Which of the following could the user do to most likely resolve the issue?

- A . Enable cellular data.
- B . Increase data limits.
- C . Disconnect the VPN.
- D . Reinstall the SIM card.

---

**Answer: A**

---

Explanation:

The most likely solution to this issue is to enable cellular data. After a business trip, the user may have disabled cellular data to avoid roaming charges, or the phone may have been set to Wi-Fi only for internet access. Enabling cellular data would restore internet access outside of Wi-Fi networks.

---

### **Question: 57**

---

A technician needs to configure a newly installed SSD. Which of the following tools should the technician use? (Select two).

- A . regedit.exe
- B . resmon.exe
- C . gpedit.msc
- D . diskmgmt.msc

- E . dfregui.exe
- F . diskpart.msc

---

**Answer: D, F**

---

Explanation:

To configure a new SSD, the technician would use diskmgmt.msc (Disk Management) and diskpart.msc (Diskpart). These tools allow for partitioning, formatting, and managing the SSD. Disk Management is a graphical utility that provides easy access to these tasks, while Diskpart is a command-line tool with advanced features for disk configuration.

Diskmgmt.msc: A GUI-based tool used to manage disk partitions.

Diskpart.msc: A command-line utility used for advanced disk configuration.

---

### **Question: 58**

---

Which of the following is natively used with Active Directory?

- A . Windows 10
- B . macOS
- C . Linux
- D . Chrome OS

---

**Answer: A**

---

Explanation:

Windows 10 is natively compatible with Active Directory. Active Directory is a Windows-based directory service that manages domain-based networks. It allows for centralized management of users, groups, and resources, which is a key feature in enterprise environments using Windows OS, such as Windows 10. Other operating systems like macOS, Linux, and Chrome OS may require additional software or configurations to interact with Active Directory, but they do not natively support it.

---

### **Question: 59**

---

A user downloaded a 64-bit version of a new software program, but the installation failed due to an error. Which of the following most likely caused the error?

- A . The OS version is incompatible.
- B . The user needs to enable ActiveX.
- C . The .NET Framework needs to be updated.
- D . The user needs administrator privileges.

---

**Answer: A**

---

Explanation:

The most likely reason for the installation failure of a 64-bit software is that the operating system is incompatible, specifically if the system is running a 32-bit version of the OS. A 64-bit program requires a 64-bit operating system to run, and if the user's OS is a 32-bit version, the software will fail to install. Other reasons, like needing administrator privileges or updating .NET, are valid but less likely since the error message would be different.

Microsoft Support: 32-bit and 64-bit Windows: Frequently Asked Questions

CompTIA A+ 220-1102 Study Guide (CompTIA) (ProfMesser)

---

**Question: 60**

---

Which of the following system preference items allows a user to enable third-party application installations on macOS 11?

- A . Keychain
- B . Privacy
- C . Accessibility
- D . Spotlight

---

**Answer: B**

---

Explanation:

In macOS, the 'Privacy' settings under 'Security & Privacy' are where users can control which applications are allowed to run, including third-party apps. By default, macOS may restrict apps that are not downloaded from the App Store, but in the Privacy settings, users can enable installations from identified developers or even from any source. The other options like 'Keychain' manage passwords and certificates, 'Accessibility' deals with assistive technologies, and 'Spotlight' is the search feature.

Apple Support: Safely open apps on your Mac

CompTIA A+ 220-1102 Study Guide (Whizlabs)

---

**Question: 61**

---

A customer needs to verify an executable file that the customer downloaded from a website. Which of the following should the customer use to verify the file?

- A . Password manager
- B . BitLocker
- C . FileVault

- D . Checksum
- E . Secure site

---

**Answer: D**

---

Explanation:

A checksum is a cryptographic hash function (like MD5 or SHA-256) used to verify the integrity of files. When downloading files from the internet, websites often provide the checksum value of the file so that users can ensure the file was not altered during download or corrupted. The user can generate the checksum on their local system and compare it to the one provided by the site. If they match, the file is intact and safe to use. Other options like BitLocker or FileVault are encryption tools, and a password manager is irrelevant to file verification.

CompTIA A+ 220-1102 Domain 3.5: File Integrity Checking (CompTIA) (ProfMesser)

---

### **Question: 62**

---

A user is unable to log in to a workstation. The user reports an error message about the date being incorrect. A technician reviews the date and verifies it is correct, but the system clock is an hour behind. The technician also determines this workstation is the only one affected. Which of the following is the most likely issue?

- A . Time drift
- B . NTP failure
- C . Windows Update
- D . CMOS battery

---

**Answer: A**

---

Explanation:

Time drift occurs when the internal clock of a computer is not properly synchronized, often leading to discrepancies like being an hour behind. In this case, the workstation is the only device affected, indicating that it's likely a local issue. Time drift can happen if the system clock isn't syncing properly with an NTP (Network Time Protocol) server or if automatic daylight savings adjustments aren't enabled. It's less likely to be a CMOS battery issue since the technician has already verified the correct date and the system clock isn't completely reset (which is what happens when the CMOS battery fails).

Troubleshooting Time Synchronization Issues in Windows (Help Desk Geek) (Zendesk)

---

### **Question: 63**

---

A technician is installing a new SOHO wireless router and wants to ensure it is secure and uses the latest network features. Which of the following should the technician do first?

- A . Disable the unused ports.

- B . Enable DHCP reservations.
- C . Update the firmware.
- D . Disable the guest account.

---

**Answer: C**

---

Explanation:

The first step in securing a newly installed SOHO (Small Office/Home Office) wireless router is to ensure it has the latest firmware installed. Firmware updates often include important security patches and new features that protect the router from known vulnerabilities. Other actions, like disabling unused ports or guest accounts, can be useful for hardening the security, but they should come after the router is running the most recent and secure version of its firmware.

CompTIA A+ Core 2 Objectives, Domain 2.1: Best Practices for Securing a SOHO Network (ProfMesser) (Whizlabs)

---

### **Question: 64**

---

Which of the following should be used to configure automatic backups on macOS?

- A . Mission Control
- B . Time Machine
- C . Disaster Recovery
- D . System Restore

---

**Answer: B**

---

Explanation:

Time Machine is the built-in backup feature for macOS that allows users to back up their system automatically. It continuously backs up everything on the Mac, including files, applications, system files, and settings, allowing users to restore their system to a previous state if needed. Time Machine operates by creating hourly backups for the past 24 hours, daily backups for the past month, and weekly backups for all previous months. Other options like 'Mission Control' help in organizing windows, while 'System Restore' is a feature more common in Windows operating systems, not macOS.

Apple Support: Use Time Machine to back up or restore your Mac

CompTIA A+ Study Guide - Backup and Recovery Concepts in macOS (Whizlabs)

---

### **Question: 65**

---

Which of the following device types would a technician consider a security concern?

- A . NIC

- B . IoT
- C . PoE
- D . LC

---

**Answer: B**

---

Explanation:

IoT (Internet of Things) devices are often considered a security concern due to their typically weak security protocols and the fact that many IoT manufacturers do not prioritize security when designing these devices. These devices often lack the capability to be regularly patched or updated, which leaves them vulnerable to exploitation by attackers. The multitude of IoT devices, such as smart thermostats, cameras, and even light bulbs, when connected to a network, can serve as entry points for cyberattacks if not secured properly. In contrast, NICs (Network Interface Cards), PoE (Power over Ethernet), and LC (a type of fiber optic connector) do not inherently pose the same level of security risk as IoT devices because they are more established technologies and typically have better security practices in place.

CompTIA A+ Exam Objectives - 220-1102, Domain 2.7: Security (CompTIA) (ProfMesser)

---

### **Question: 66**

---

A customer recently upgraded their computer to the latest Windows version and is now having issues with the display. The icons and text are too large, and the colors are not accurate. Which of the following Control Panel options should the technician adjust to help the customer?

- A . Ease of Access
- B . Device Manager
- C . Network and Sharing Center
- D . Programs and Features

---

**Answer: B**

---

Explanation:

When a customer experiences display issues such as large icons and inaccurate colors after a Windows upgrade, the most appropriate Control Panel option to address these issues is 'Device Manager.' The technician can use Device Manager to check and update display drivers, which are often the cause of such problems after an OS upgrade. Updating or reinstalling the correct drivers can help resolve display resolution and color issues.

- A . Ease of Access focuses on accessibility features and does not directly address display driver issues.
- C . Network and Sharing Center is related to network settings and does not affect display settings.
- D . Programs and Features is used for managing installed programs and features but is not relevant for updating display drivers.

### **Question: 67**

---

Which of the following environmental effects can be the result of using virtualization?

- A . Greater energy consumption
- B . Noise pollution
- C . Reduced space requirements
- D . Fewer maintenance needs

---

**Answer: C**

---

Explanation:

One of the key environmental benefits of using virtualization is the reduction in physical space requirements. Virtualization allows multiple virtual machines to run on a single physical server, reducing the need for multiple physical servers. This consolidation leads to fewer physical machines, saving space in data centers and reducing the overall physical footprint.

- A . Greater energy consumption is incorrect as virtualization typically leads to reduced energy consumption due to the consolidation of hardware.
- B . Noise pollution can be reduced because fewer physical machines often mean less overall noise.
- D . Fewer maintenance needs is a possible benefit but not directly related to environmental effects like reduced space requirements.

CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.5: Summarizing environmental impacts and local environmental controls, including the benefits of virtualization.

---

### **Question: 68**

---

A technician needs to import a new digital certificate and place it in the proper location. Which of the following Control Panel utilities should the technician use to import the certificate?

- A . Internet Options
- B . Network and Sharing Center
- C . Credential Manager
- D . Security and Maintenance

---

**Answer: A**

---

Explanation:

To import a new digital certificate and place it in the proper location, the technician should use the 'Internet Options' utility in the Control Panel. This utility allows users to manage various settings related to internet connections and security, including the import and management of digital certificates under the 'Content' tab.

B . Network and Sharing Center is used for managing network connections and sharing settings but not for managing digital certificates.

C . Credential Manager is used to store and manage login credentials for websites and applications but not for importing digital certificates.

D . Security and Maintenance provides an overview of the security and maintenance status of the system but does not directly handle digital certificate management.

CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 1.4: Using Control Panel utilities including Internet Options for managing digital certificates.

---

### Question: 69

---

An application is not performing well and will occasionally shut down with no error provided. Which of the following Task Manager tabs should be used to troubleshoot the application while it is active?

- A . Users
- B . Services
- C . Performance
- D . Startup

---

**Answer: C**

---

Explanation:

When troubleshooting an application that is not performing well and occasionally shuts down with no error, the 'Performance' tab in Task Manager is the most appropriate tool to use. This tab provides real-time data on CPU, memory, disk, and network usage, which can help identify resource bottlenecks or spikes that could be causing the application to malfunction. Monitoring these metrics while the application is running can offer insights into whether the issue is related to system resources.

A . Users tab shows which users are currently logged into the system and their resource usage but does not provide detailed performance metrics for troubleshooting application issues.

B . Services tab shows the status of background services but does not provide direct information about the application's performance.

D . Startup tab manages which applications start with Windows and their impact on startup time but is not useful for monitoring active application performance.

CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 1.3: Using features and tools of the Microsoft Windows OS, including Task Manager's Performance tab.

---

## **Question: 70**

---

A technician is assisting a customer who is having difficulty accessing the company's website. Which of the following should the technician do first?

- A . Ask the customer for their log-in credentials.
- B . Check the company's internal knowledge base for solutions.
- C . Refer the customer to a more experienced technician.
- D . Record the details of the issue in the company's ticketing system.

---

**Answer: D**

---

Explanation:

When a customer is having difficulty accessing the company's website, the technician should first document the issue in the company's ticketing system. This step ensures that the problem is officially logged, which allows for proper tracking, prioritization, and assignment to the appropriate personnel if needed. Recording the details helps in maintaining a record of the issue and the troubleshooting steps taken, which is useful for future reference and analysis.

- A . Ask the customer for their log-in credentials. This is not appropriate as it breaches security protocols and is not the first step in troubleshooting.
- B . Check the company's internal knowledge base for solutions. While useful, this step comes after the issue has been documented.
- C . Refer the customer to a more experienced technician. This might be necessary later, but initially, the issue should be documented.

CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.1: Documentation and support systems, including the use of ticketing systems for tracking incidents.

---

## **Question: 71**

---

The camera and microphone on an iPhone user's device are activating without any user input. The user's friend recently modified the device to allow applications to be installed outside the normal App Store. Which of the following is the issue?

- A . The user connected a counterfeit Lightning cable to the iPhone.
- B . The device is unenrolled from Mobile Device Management.
- C . The device was jailbroken to remove internal security protections.
- D . The iPhone has an out-of-date operating system.

---

**Answer: C**

---

Explanation:

The camera and microphone on an iPhone activating without user input, especially after allowing applications to be installed outside the normal App Store, is a classic sign of the device being jailbroken. Jailbreaking an iPhone removes many of the built-in security features and restrictions, allowing the installation of apps from third-party sources. These third-party apps can be malicious and can gain unauthorized access to system resources like the camera and microphone.

- A . The user connected a counterfeit Lightning cable to the iPhone. While counterfeit cables can be harmful, they typically cause charging or connectivity issues rather than security vulnerabilities that would enable camera and microphone activation without user input.
- B . The device is unenrolled from Mobile Device Management. Unenrolling from MDM removes organizational controls but does not directly cause unauthorized camera and microphone activation.
- D . The iPhone has an out-of-date operating system. An outdated OS can have vulnerabilities, but the scenario specifically mentions modifications to allow third-party app installations, pointing to jailbreaking as the primary cause.

CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 2.3: Security measures and their purposes including mobile device security.

---

### **Question: 72**

---

Which of the following Windows 10 editions is the most cost-effective and appropriate for a single user who needs to access their computer remotely?

- A . Education
- B . Pro
- C . Enterprise
- D . Home

---

**Answer: B**

---

Explanation:

For a single user who needs to access their computer remotely, the Windows 10 Pro edition is the most cost-effective and appropriate choice. It includes features such as Remote Desktop, which are essential for remote access.

Option A: Education This edition is designed for academic institutions and includes educational features. It is not the most cost-effective for a single user.

Option B: Pro Windows 10 Pro includes Remote Desktop and other business features. It is suitable and cost-effective for single users needing remote access.

Option C: Enterprise This edition includes advanced features for large organizations and is more expensive, making it less cost-effective for a single user.

Option D: Home While cost-effective, Windows 10 Home does not include the Remote Desktop feature, making it unsuitable for this requirement.

CompTIA A+ 220-1102 Objective 1.1 (Identify basic features of Microsoft Windows editions), particularly comparing editions based on features and cost.

---

### Question: 73

---

A technician is investigating a workstation that has not received the latest policy changes. Which of the following commands should the technician use to apply the latest domain policy changes?

- A . sfc /scannow
- B . gpupdate /force
- C . chkdsk /y
- D . xcopy Zp

---

**Answer: B**

---

Explanation:

When a workstation has not received the latest policy changes, the gpupdate command is used to manually apply the latest group policies from the domain controller.

Option A: sfc /scannow This command is used to scan and repair corrupted system files, not to update group policies.

Option B: gpupdate /force This command forces the workstation to reapply all group policies, ensuring that the latest policies are applied immediately.

Option C: chkdsk /y This command checks the integrity of the file system and fixes logical file system errors, not to update group policies.

Option D: xcopy /Zp This command is used for copying files and directories, not for updating group policies.

CompTIA A+ 220-1102 Objective 1.6 (Configure Microsoft Windows networking features on a client/desktop), particularly managing and applying group policies.

---

### Question: 74

---

Which of the following filesystems supports journaling?

- A . NTFS
- B . exFAT
- C . HFS
- D . ext2

---

**Answer: A**

---

Explanation:

Journaling is a feature that helps maintain the integrity of the filesystem by keeping a record of changes not yet committed to the main file system. This feature is supported by various filesystems, but not all.

Option A: NTFS NTFS (New Technology File System) is a filesystem used by Windows that supports journaling. This makes it resilient to corruption from unexpected shutdowns or crashes by keeping a log of file changes.

Option B: exFAT exFAT (Extended File Allocation Table) does not support journaling. It is optimized for flash drives and large files but lacks advanced features like journaling.

Option C: HFS HFS (Hierarchical File System) is an older filesystem used by Apple. HFS+ (also known as Mac OS Extended) supports journaling, but HFS itself does not.

Option D: ext2 ext2 (Second Extended File System) is a filesystem for Linux that does not support journaling. Its successor, ext3, introduced journaling.

CompTIA A+ 220-1102 Objective 1.8 (Explain common OS types and their purposes), particularly filesystems and their features.

---

### Question: 75

---

Which of the following provides disk encryption on computers running a Windows OS?

- A . FileVault
- B . BitLocker
- C . Private Key
- D . PowerShell

---

### Answer: B

---

Explanation:

BitLocker is a full-disk encryption feature included with certain editions of Windows, designed to protect data by providing encryption for entire volumes.

Option A: FileVault FileVault is a disk encryption program in macOS, not Windows.

Option B: BitLocker BitLocker is the correct tool for disk encryption on Windows operating systems, providing full disk encryption.

Option C: Private Key A private key is part of public key infrastructure (PKI) used in encryption, but it is not a tool for disk encryption by itself.

Option D: PowerShell PowerShell is a task automation and configuration management framework from Microsoft, not a tool for disk encryption.

CompTIA A+ 220-1102 Objective 2.5 (Manage and configure basic security settings in the Windows OS), particularly BitLocker for disk encryption.

---

### Question: 76

---

The company uses shared drives as part of a workforce collaboration process. To ensure the correct access permissions, inheritance at the top-level folder is assigned to each department. A manager's team is working on confidential material and wants to ensure only the immediate team can view a specific folder and its subsequent files and subfolders. Which of the following actions should the technician most likely take?

- A . Turn off inheritance on the requested folder only and set the requested permissions to each file manually.
- B . Turn off inheritance at the top-level folder and remove all inherited permissions.
- C . Turn off Inheritance at the top-level folder and set permissions to each file and subfolder manually.
- D . Turn off inheritance on the requested folder only, set the requested permissions, and then turn on inheritance under the child folders.

---

**Answer: D**

---

Explanation:

For managing permissions where a specific folder needs to have different access controls than its parent, turning off inheritance for that specific folder is the correct approach.

Option A: Turn off inheritance on the requested folder only and set the requested permissions to each file manually  
This is partially correct, but setting permissions manually for each file is inefficient and error-prone.

Option B: Turn off inheritance at the top-level folder and remove all inherited permissions This action would disrupt permissions for all other folders and files, not just the confidential folder.

Option C: Turn off inheritance at the top-level folder and set permissions to each file and subfolder manually This approach is overly broad and inefficient, impacting more than just the specific folder that needs restricted access.

Option D: Turn off inheritance on the requested folder only, set the requested permissions, and then turn on inheritance under the child folders This ensures the specific folder has unique permissions while allowing those permissions to propagate to its children, maintaining security and ease of management.

CompTIA A+ 220-1102 Objective 2.5 (Manage and configure basic security settings in the Windows OS), particularly file and folder permissions and inheritance settings.

---

### **Question: 77**

---

A workstation does not recognize a printer. However, the previous day. the printer successfully received a job from the workstation. Which of the following tools should a technician use to see what happened before the failure?

- A . Performance Monitor
- B . Devices and Printers
- C . Task Scheduler
- D . Event Viewer

---

**Answer: D**

---

Explanation:

When troubleshooting a printer that was previously working but is no longer recognized by a workstation, Event Viewer is the most appropriate tool to check for historical logs and events related to the printer and the system.

Option A: Performance Monitor Performance Monitor is used for monitoring system performance and resources in real-time and does not provide specific historical event logs related to device failures.

Option B: Devices and Printers Devices and Printers show the status and properties of connected devices but do not provide a historical log of events or errors.

Option C: Task Scheduler Task Scheduler manages and monitors scheduled tasks but does not log hardware events or errors.

Option D: Event Viewer Event Viewer logs system events, including errors, warnings, and information related to hardware and software. It is ideal for checking what happened prior to the printer failure.

CompTIA A+ 220-1102 Objective 3.1 (Troubleshoot common Windows OS problems), particularly using Event Viewer for diagnosing issues.

---

### **Question: 78**

---

A user's Android phone has been randomly restarting. A technician investigates and finds several applications have been installed that are not available within the standard marketplace. Which of the following is most likely the cause of the issue?

- A . The OS update failed.
- B . The user downloaded malware.
- C . The device is In developer mode.
- D . The over-the-air carrier update failed.

---

### **Answer: B**

---

Explanation:

Random restarting of an Android phone and the presence of applications not from the standard marketplace strongly suggest the possibility of malware.

Option A: The OS update failed While an OS update failure can cause issues, it is less likely to result in random restarts compared to malware.

Option B: The user downloaded malware Malware is a common cause of erratic behavior, including random restarts, especially when applications are installed from unofficial sources.

Option C: The device is in developer mode Developer mode alone does not typically cause random restarts. It may make the device more susceptible to issues if improper apps are installed.

Option D: The over-the-air carrier update failed Similar to the OS update, this would more likely cause consistent issues rather than random restarts.

CompTIA A+ 220-1102 Objective 2.3 (Detect, remove, and prevent malware) and Objective 3.5 (Mobile OS and application security issues).

---

### Question: 79

---

A technician is configuring security for a computer that is located in a common area.

a. A sign above the computer indicates only authorized users can use the computer. Guests visiting the office must walk past the computer to enter and leave the office. Which of the following will offer the best protection against physical threats?

- A . Using screen lock
- B . Installing a privacy screen
- C . Implementing password complexity
- D . Locking the computer case
- E . Enabling drive encryption

---

**Answer: D**

---

Explanation:

The best protection against physical threats, especially in a common area where the computer is publicly accessible, involves physically securing the hardware.

Option A: Using screen lock Screen locks are good for securing access temporarily but do not protect against physical tampering or theft.

Option B: Installing a privacy screen Privacy screens prevent visual access but do not secure the hardware.

Option C: Implementing password complexity Password complexity helps secure digital access but does not prevent physical threats.

Option D: Locking the computer case Physically securing the case prevents unauthorized individuals from tampering with internal components or stealing the computer.

Option E: Enabling drive encryption Encryption protects data but does not prevent physical access to the hardware itself.

CompTIA A+ 220-1102 Objective 2.1 (Physical security), particularly physical security measures like locking the computer case.

---

### Question: 80

---

A user is unable to access the company's internal network on a separate subnet. A help desk technician verifies the user's credentials, and the user has the appropriate permissions to access the network. The technician checks the network and finds the connection is stable. No other users are having this issue. Which of the following should the technician do next?

- A . Consult with the firewall team to see if the user's IP address is blocked.

- B . Delete the user's credentials and create new ones.
- C . Run a virus scan on the user's workstation.
- D . Update the network drivers on the user's workstation.

---

**Answer: A**

---

Explanation:

In this scenario, the user cannot access a separate subnet, and all other checks (credentials, network stability, and permissions) have been verified. The next logical step is to check if the user's IP address is being blocked by a firewall.

Option A: Consult with the firewall team to see if the user's IP address is blocked. Firewalls can block specific IP addresses, preventing access to certain network segments. Given the problem's nature and the steps already taken, this is the most logical next step to ensure the user's IP is not inadvertently blocked.

Option B: Delete the user's credentials and create new ones. This step is unnecessary since the credentials have already been verified as correct.

Option C: Run a virus scan on the user's workstation. While important for overall security, a virus scan is unlikely to resolve an issue specific to accessing a subnet if the problem does not affect other users.

Option D: Update the network drivers on the user's workstation. If the network connection is stable and the issue is isolated to accessing a specific subnet, network drivers are unlikely to be the cause.

CompTIA A+ 220-1102 Objective 2.0 (Security), particularly firewall settings.

---

### **Question: 81**

---

A company's help desk receives numerous calls from employees reporting issues related to a current security breach. Which of the following steps should the help desk team take to document the breach?

- A . Record the details in the ticketing system.
- B . Take screenshots and attach them to the root cause analysis.
- C . Discuss the incident with the company's legal team.
- D . List the details in the company's knowledge base.

---

**Answer: A**

---

Explanation:

In the event of a security breach, documenting the incident is crucial for tracking, analysis, and resolution. The appropriate steps should ensure thorough documentation and communication:

Option A: Record the details in the ticketing system. Correct Answer. The ticketing system is the primary tool for IT support to track incidents. Recording the details in the ticketing system ensures that all relevant information is documented systematically, can be easily accessed, and tracked through the resolution process.

This aligns with best practices in incident documentation and support systems information management as outlined in the CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.1.

Option B: Take screenshots and attach them to the root cause analysis. While screenshots can be useful, the first step should be to record the details in the ticketing system. Screenshots may be added later as supplementary information.

Option C: Discuss the incident with the company's legal team. Involving the legal team is important for certain aspects of a security breach, but the initial step should still be to document the incident in the ticketing system.

---

### **Question: 82**

---

After a computer upgrade at an imaging lab, the upgraded computers are not able to obtain an IP address. Which of the following is most likely the issue?

- A . The switch is only providing IPv6 addresses.
- B . The OS must be updated to be compatible with the imaging software.
- C . The switch has port security enabled.
- D . The switch does not support multicast traffic.

---

### **Answer: C**

---

Explanation:

When upgraded computers are not able to obtain an IP address, the issue often lies in the network configuration. Here's a detailed explanation:

Option A: The switch is only providing IPv6 addresses. This is unlikely because if the switch were providing IPv6 addresses, the devices would still receive an IP address, albeit an IPv6 one. The issue described indicates no IP address is being obtained at all.

Option B: The OS must be updated to be compatible with the imaging software. This option is unrelated to obtaining an IP address. Compatibility with imaging software would not prevent the devices from getting an IP address.

Option C: The switch has port security enabled. Correct Answer. Port security on a switch restricts access based on MAC addresses. If the MAC addresses of the upgraded computers are not recognized or have not been added to the allowed list, the switch will not provide network access, resulting in the computers not obtaining an IP address.

Option D: The switch does not support multicast traffic. This is unrelated to obtaining an IP address. Multicast traffic deals with specific types of network communication and would not affect the basic DHCP IP address assignment process.

---

### **Question: 83**

---

The user often hosts meetings from a Windows desktop, and meeting participants ask the user to make the text larger when the user shares the computer screen. When not in meetings, the user wants the text to be smaller for work tasks. Which of the following is the most efficient way to change text font size?

- A . Issuing a laptop to the user with increased font size to be used only for meetings
- B . Using display settings to adjust the text size during meetings

- C . Adding a local user account, which has a larger font size set, for the user to log in to during meetings
- D . Adding a second monitor to the user's desktop and increase the font size for only that display

---

**Answer: B**

---

Explanation:

Changing the text size efficiently for different scenarios, such as meetings and regular work tasks, can be managed directly through the Windows display settings. This method is both quick and easily reversible, making it the most efficient solution compared to the other options provided.

Option A: Issuing a laptop to the user with increased font size to be used only for meetings This option is not efficient as it requires additional hardware and setup time, which is impractical for simply adjusting text size.

Option B: Using display settings to adjust the text size during meetings Correct Answer. Windows provides built-in functionality to adjust the text size on the display. This can be accessed via:

Windows Settings > System > Display.

Under 'Scale and layout,' you can change the size of text, apps, and other items. This method allows for quick changes and can be reverted just as quickly after meetings.

Option C: Adding a local user account, which has a larger font size set, for the user to log in to during meetings This approach involves additional steps of logging out and logging back in, which is less efficient than simply adjusting the display settings.

Option D: Adding a second monitor to the user's desktop and increase the font size for only that display While this can be a solution, it is not the most efficient way as it involves additional hardware and configuration. It's more suited for scenarios requiring constant dual-display use rather than just changing text size occasionally.

---

### **Question: 84**

---

A user is attempting to access a shared drive from a company-issued laptop while working from home. The user is unable to access any files and notices a red X next to each shared drive. Which of the following needs to be configured in order to restore the user's access to the shared drives?

- A . IPv6
- B . VPN
- C . IPS
- D . DNS

---

**Answer: B**

---

Explanation:

When a user is unable to access shared drives from a company-issued laptop while working from home, the likely requirement is:

VPN (Virtual Private Network): A VPN allows secure access to the company's network from a remote location. Without a VPN connection, the user cannot access network resources such as shared drives.

IPv6: Involves IP addressing and is not directly related to accessing shared drives.

IPS (Intrusion Prevention System): Provides network security but does not facilitate access to shared drives.

DNS: Manages domain name resolution and is not typically the issue when specific shared drives are inaccessible.

CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Explain common methods for securing mobile and embedded devices.

VPN configuration and remote access documentation.

---

### **Question: 85**

---

A customer is configuring on an old desktop an inexpensive file server to share photos and videos and wants to avoid complicated licensing. Which of the following operating systems should the technician most likely recommend?

- A . Chrome OS
- B . Linux
- C . macOS
- D . Windows

---

**Answer: B**

---

Explanation:

For an inexpensive file server to share photos and videos while avoiding complicated licensing, the technician should recommend:

Linux: Linux is a free and open-source operating system that is ideal for setting up a file server. It offers robust file-sharing capabilities with minimal licensing complications.

Chrome OS: Designed primarily for lightweight, web-based tasks and not ideal for a file server.

macOS: Requires Apple hardware and involves more complex licensing compared to Linux.

Windows: While capable of being a file server, Windows may involve licensing fees, particularly for server editions.

CompTIA A+ 220-1102 Exam Objectives, Section 1.8: Explain common OS types and their purposes.

Linux documentation and its use in setting up file servers.

---

### **Question: 86**

---

A technician, who is completing hardware upgrades at a company, is approached by a user who submitted a computer upgrade request. After checking the list of offices to upgrade, the technician finds that the user's office is

not listed for an upgrade. Which of the following actions should the technician take next?

- A . Ask the company's human resources department to address the issue.
- B . Notify the project manager about the user's concern.
- C . Tell the user that this request is not on the list to be upgraded.
- D . Ask the user's supervisor if the technician should upgrade the computer.

---

**Answer: B**

---

Explanation:

When a technician finds that a user's office is not listed for an upgrade but the user has submitted a request, the appropriate action is to:

Notify the project manager about the user's concern: The project manager oversees the upgrade process and can address any discrepancies or omissions in the upgrade list.

Ask the company's human resources department to address the issue: HR typically handles personnel matters, not hardware upgrades.

Tell the user that this request is not on the list to be upgraded: This does not resolve the user's concern and could cause frustration.

Ask the user's supervisor if the technician should upgrade the computer: The supervisor may not have the authority or information to make decisions about the upgrade list.

CompTIA A+ 220-1102 Exam Objectives, Section 4.1: Given a scenario implement best practices associated with documentation and support systems information management.

Best practices for handling user requests and project management documentation.

---

### **Question: 87**

---

Employees want their Windows 10 laptops to wirelessly connect when they take them home. Which of the following should the employees configure so the laptops can automatically connect wirelessly?

- A . Network and Internet settings
- B . Windows Firewall settings
- C . Devices and Printers
- D . Personalization settings

---

**Answer: A**

---

Explanation:

To ensure that Windows 10 laptops can automatically connect to Wi-Fi networks when employees take them home, the appropriate configuration is:

**Network and Internet settings:** These settings allow users to manage Wi-Fi connections, configure automatic connections to known networks, and manage network profiles.

Go to Settings > Network & Internet > Wi-Fi.

Ensure the option to connect automatically to the home Wi-Fi network is enabled.

**Windows Firewall settings:** These are used to manage firewall rules and do not control Wi-Fi connectivity.

**Devices and Printers:** Used for managing connected devices and printers, not for network connections.

**Personalization settings:** These settings are for customizing the appearance of the Windows interface and do not affect network connections.

CompTIA A+ 220-1102 Exam Objectives, Section 1.6: Given a scenario configure Microsoft Windows networking features on a client/desktop.

Windows network configuration documentation.

---

### **Question: 88**

---

A technician is implementing the latest application security updates for endpoints on an enterprise network. Which of the following solutions should the technician use to ensure device security on the network while adhering to industry best practices?

- A . Automate the patching process.
- B . Monitor the firewall configuration.
- C . Implement access control lists.
- D . Document all changes.

---

### **Answer: A**

---

Explanation:

To ensure device security on the network while adhering to industry best practices, the technician should:

**Automate the patching process:** This ensures that all devices receive the latest security updates in a timely manner without manual intervention, reducing the risk of vulnerabilities.

**Monitor the firewall configuration:** Important for network security but does not directly ensure all devices are patched.

**Implement access control lists:** Controls access to resources but does not ensure devices are patched.

**Document all changes:** Important for change management but does not directly impact the patching process.

CompTIA A+ 220-1102 Exam Objectives, Section 2.6: Given a scenario configure a workstation to meet best practices for security.

Best practices for application security updates and patch management.

---

### Question: 89

---

Which of the following ensures data is unrecoverable on a lost or stolen mobile device?

- A . Device encryption
- B . Remote wipe
- C . Data backup
- D . Fingerprint reader

---

**Answer: B**

---

Explanation:

To ensure data is unrecoverable on a lost or stolen mobile device, the best solution is:

Remote wipe: This feature allows the device owner or IT administrator to remotely erase all data on the device, ensuring that it cannot be recovered by unauthorized users.

Device encryption: While important for protecting data, encryption alone does not remove data from the device.

Data backup: Ensures data is saved elsewhere but does not make it unrecoverable on the lost or stolen device.

Fingerprint reader: Provides security for accessing the device but does not affect data recovery if the device is compromised.

CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Explain common methods for securing mobile and embedded devices.

Mobile device security practices documentation.

---

### Question: 90

---

After a user upgraded the Windows operating system to the latest feature release, the user notices that one of the legacy applications that was running correctly before the upgrade does not open some windows and is only partially functional. Which of the following actions should the user take to troubleshoot the issue?

- A . Run the application as Administrator.
- B . Raise the User Account Control level.
- C . Turn off Windows Defender Firewall.
- D . Disable compatibility mode for the application.

---

**Answer: A**

---

Explanation:

When a legacy application is not fully functional after upgrading the Windows operating system, the first step to troubleshoot the issue is to:

Run the application as Administrator: Legacy applications often require administrative privileges to run correctly. Running the application with these privileges can resolve issues related to permissions and access to certain system resources.

Raise the User Account Control level: This increases security prompts but does not resolve compatibility issues.

Turn off Windows Defender Firewall: This can expose the system to security risks and is unlikely to resolve application functionality issues.

Disable compatibility mode for the application: Compatibility mode should generally be enabled for legacy applications to ensure they run properly on newer OS versions.

CompTIA A+ 220-1102 Exam Objectives, Section 1.3: Given a scenario use features and tools of the Microsoft Windows 10 operating system (OS).

Windows application compatibility troubleshooting documentation.

---

### Question: 91

---

An organization's critical database files were attacked with ransomware. The company refuses to pay the ransom for a decryption key. All traces of the infection have been removed from the underlying servers. Which of the following should the company do next?

- A . Scan all of the infected files with up-to-date, anti-malware cleaning software.
- B . Fully patch the server operating systems hosting the fileshares.
- C . Change the files to be read-only.
- D . Restore critical data from backup.

---

### Answer: D

---

Explanation:

When an organization refuses to pay the ransom for a decryption key after a ransomware attack, and all traces of the infection have been removed, the next critical step is:

Restore critical data from backup: This is the most effective way to recover from a ransomware attack without paying the ransom. Assuming the organization has good backup practices, the backups should be free from infection and can be restored to get the systems operational again.

Scan all of the infected files with up-to-date, anti-malware cleaning software: This step is important during the infection removal process but does not address restoring the encrypted files.

Fully patch the server operating systems hosting the fileshares: While this is necessary to prevent future attacks, it does not recover the encrypted files.

Change the files to be read-only: This will not help recover the encrypted data.

CompTIA A+ 220-1102 Exam Objectives, Section 2.8: Given a scenario use common data destruction and disposal methods.

Best practices for ransomware recovery.

---

### Question: 92

---

A user reports that a device with a statically defined IP is unable to connect to the internet. The technician runs the ipconfig /all command and sees the following output:

IPv4 Address..... 192.168.0.74

Subnet Mask.....255.255.255.255

Default Gateway..... 192.168.0.1

Which of the following is most likely the reason for the issue?

- A . The default gateway is up.
- B . The user has an APIPA IP address.
- C . The IP address is on the wrong subnet
- D . The subnet mask is incorrect.

---

### Answer: D

---

Explanation:

The ipconfig /all output shows the following:

IPv4 Address..... 192.168.0.74 Subnet Mask..... 255.255.255.255 Default Gateway..... 192.168.0.1

The issue with the subnet mask being set to 255.255.255.255 is that it specifies a single host subnet, meaning the device cannot communicate with other devices on the network or access the internet. The correct subnet mask for a typical home network should be:

Subnet mask of 255.255.255.0: This allows for communication within the same local network (192.168.0.0/24).

Default gateway 192.168.0.1: Correct, this is the typical address for the router.

IPv4 Address 192.168.0.74: Correct, within the correct subnet range.

Changing the subnet mask to 255.255.255.0 will resolve the connectivity issue.

CompTIA A+ 220-1102 Exam Objectives, Section 2.5: Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

IP addressing and subnetting documentation.

---

### **Question: 93**

---

A user accidentally installed the incorrect word processing application on an iMac. Which of the following would allow the user to uninstall the incorrect application?

- A . Move the application to the desktop and press delete.
- B . Identify the application in Finder and drag it to the trash can.
- C . Use Spotlight to search for the application, and then run the application.
- D . Use Time Machine to go back to the date before the installation.

---

**Answer: B**

---

Explanation:

To uninstall an incorrect application on an iMac, the standard and recommended method is:

Identify the application in Finder and drag it to the trash can: This action removes the application from the system. After dragging the application to the trash, the user should empty the trash to complete the uninstallation.

Move the application to the desktop and press delete: This action does not uninstall the application.

Use Spotlight to search for the application, and then run the application: Running the application does not uninstall it.

Use Time Machine to go back to the date before the installation: This method can be used to restore the system to a previous state but is not necessary for uninstalling an application.

CompTIA A+ 220-1102 Exam Objectives, Section 1.10: Identify common features and tools of the macOS/desktop OS.

Apple support documentation for uninstalling applications.

---

### **Question: 94**

---

A technician assigns the equivalent of root-level permissions to a user to perform a task. Which of the following user roles within the Windows OS should the technician choose?

- A . Power
- B . Default
- C . Administrator
- D . Superuser

---

**Answer: C**

---

Explanation:

In the Windows OS, to grant a user permissions equivalent to root-level permissions (which means full control over the system), the user needs to be given:

**Administrator:** The Administrator role provides full control over the system, including the ability to install and uninstall software, change system settings, and access all files and directories.

**Power:** The Power User role provides some administrative capabilities but not full control. It is a legacy role with fewer permissions than Administrator.

**Default:** This refers to a standard user account with limited permissions.

**Superuser:** This term is more commonly associated with Unix/Linux systems and is not a specific role in Windows.

CompTIA A+ 220-1102 Exam Objectives, Section 2.5: Given a scenario manage and configure basic security settings in the Microsoft Windows OS.

Windows user roles and permissions documentation.

---

### **Question: 95**

---

A systems administrator needs to access a hypervisor that went offline. After doing a port scan, the administrator notices that company policy is blocking the RDP default port. Which of the following ports should the administrator use to access the machine?

- A . 22
- B . 23
- C . 80
- D . 3090

---

### **Answer: A**

---

Explanation:

When a systems administrator needs to access a hypervisor and the default RDP port (3389) is blocked by company policy, the administrator can use an alternative method. One common alternative is using SSH:

Port 22: This is the default port for SSH (Secure Shell), which is commonly used for secure remote access to servers and hypervisors, especially in Unix/Linux environments.

Port 23: This is the default port for Telnet, which is an unsecured protocol and generally not recommended for remote access due to security concerns.

Port 80: This is the default port for HTTP, used for web traffic, not remote access.

Port 3090: This is not a standard port for remote access protocols.

Using SSH (port 22) is a secure and widely accepted method for remote management of servers and hypervisors.

CompTIA A+ 220-1102 Exam Objectives, Section 2.6: Compare and contrast network services and protocols.

SSH and remote access documentation.

---

## **Question: 96**

---

An employee utilizes a personal smartphone to work remotely. The employee is unable to reach the portal using the company-provided VPN service. Which of the following describes the cause of the issue?

- A . The application must be purchased by the company.
- B . The smartphone is not on the latest OS version.
- C . The smartphone is not enrolled in MDM service.
- D . The application fails to install and launch.

---

**Answer: C**

---

Explanation:

When an employee is unable to access the company portal using a VPN on their personal smartphone, the most likely cause is:

The smartphone is not enrolled in MDM service: Mobile Device Management (MDM) services often control access to company resources. If the smartphone is not enrolled, it may be blocked from accessing the VPN and, consequently, the company portal.

The application must be purchased by the company: Unlikely, as most VPN applications are free to download or included in the company's software package.

The smartphone is not on the latest OS version: While this could cause compatibility issues, it is less likely than the MDM enrollment issue.

The application fails to install and launch: This would be a different problem and would usually present specific error messages.

CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Explain common methods for securing mobile and embedded devices.

MDM configuration and access control documentation.

---

## **Question: 97**

---

A user reports the following issues:

- \* Their computer is constantly running slowly.
- \* The default home page of the web browser has changed to a suspicious search engine.
- \* They have been receiving pop-up ads on the screen.

Which of the following should a technician do first to address these issues?

- A . Update the antivirus program and run a full system scan.
- B . Uninstall the suspicious search engine and reset the home page.
- C . Install the latest updates for the operating system.

D . Block the pop-up ads using the web browser settings.

---

**Answer: A**

---

Explanation:

When a user reports slow performance, a changed home page, and pop-up ads, these are classic signs of malware infection. The first step should be:

Update the antivirus program and run a full system scan: This helps identify and remove any malware present on the system, addressing the root cause of the issues.

Uninstall the suspicious search engine and reset the home page: This addresses the symptom but not the underlying cause, which is likely malware.

Install the latest updates for the operating system: Important for security but secondary to removing malware.

Block the pop-up ads using the web browser settings: Again, addresses the symptom but not the root cause.

CompTIA A+ 220-1102 Exam Objectives, Section 3.3: Given a scenario use best practice procedures for malware removal.

Malware identification and removal documentation.

---

### **Question: 98**

---

Users report that a network printer intermittently goes offline during the day. Which of the following commands should the technician use to confirm whether the printer has connectivity issues?

- A . ping
- B . netstat
- C . net
- D . nslookup

---

**Answer: A**

---

Explanation:

To confirm whether a network printer has connectivity issues, the technician should use:

ping: This command checks the connectivity to the printer by sending packets and measuring the response time. It helps determine if the printer is reachable on the network.

netstat: Provides statistics and current network connections but does not directly confirm connectivity to a specific device.

net: Used for network resources management but not specifically for checking connectivity.

nslookup: Used for querying DNS to obtain domain name or IP address mapping, not for checking connectivity.

CompTIA A+ 220-1102 Exam Objectives, Section 2.8: Given a scenario, use networking tools.

Network troubleshooting commands documentation.

---

### **Question: 99**

---

A customer needs to purchase a desktop capable of rendering video. Which of the following should the customer prioritize?

- A . NIC
- B . USB
- C . GPU
- D . HDMI

---

**Answer: C**

---

Explanation:

For rendering video, the most critical component a customer should prioritize in a desktop is:

**GPU (Graphics Processing Unit):** The GPU is specifically designed to handle complex graphics and video rendering tasks. A powerful GPU will significantly improve performance in video rendering applications.

**NIC (Network Interface Card):** Important for network connectivity but irrelevant for video rendering.

**USB:** Useful for peripherals but does not impact video rendering capabilities.

**HDMI:** An important output interface for connecting monitors but not crucial for the rendering process itself.

CompTIA A+ 220-1102 Exam Objectives, Section 1.8: Explain common OS types and their purposes, including hardware components for specific tasks.

GPU importance in video rendering documentation.

---

### **Question: 100**

---

When a user is in the office, web pages are loading slowly on the user's phone. Which of the following best explains this issue?

- A . Exceeded the data usage limit
- B . Sluggish response time
- C . Degraded network service
- D . High network traffic

---

**Answer: D**

---

Explanation:

When a user experiences slow web page loading on their phone while in the office, the most likely cause is:

High network traffic: In an office environment, many devices are often connected to the network simultaneously, which can lead to congestion and slow internet speeds. High network traffic means more devices are competing for the same bandwidth, causing delays.

Exceeded the data usage limit: This typically applies to cellular data plans, not Wi-Fi in an office setting.

Sluggish response time: This is a symptom rather than a cause and can result from high network traffic.

Degraded network service: While this could be a factor, it is broader and less specific than high network traffic, which is more directly related to the user's experience.

CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Given a scenario troubleshoot problems with wired and wireless networks.

Network performance troubleshooting documentation.

---

### Question: 101

---

An administrator's change was approved by the change management review board. Which of the following should the administrator do next?

- A . Perform risk analysis.
- B . Assign a change coordinator.
- C . Implement the change.
- D . Verify testing results.

---

**Answer: C**

---

Explanation:

Once a change has been approved by the change management review board, the next step is to:

Implement the change: This involves carrying out the approved change in the system or environment according to the change plan.

Perform risk analysis: This should be done before the change is approved to assess potential impacts.

Assign a change coordinator: This role should be designated earlier in the process to oversee the change implementation.

Verify testing results: This should have been done before seeking approval from the review board.

CompTIA A+ 220-1102 Exam Objectives, Section 4.2: Explain basic change-management best practices.

Change management process documentation.

---

## **Question: 102**

---

Which of the following documents in criminal proceedings must be updated every time a piece of evidence is touched or transferred in order for the evidence to be considered valid?

- A . Licensing agreement
- B . Regulatory compliance
- C . Incident documentation
- D . Chain of custody

---

**Answer: D**

---

Explanation:

In criminal proceedings, maintaining the integrity of evidence is crucial. The document that must be updated every time evidence is handled or transferred is:

Chain of custody: This document tracks the history of the evidence, detailing every person who has handled it and every transfer that has occurred. It ensures that the evidence has not been tampered with and maintains its validity in court.

Licensing agreement: Pertains to software usage rights and has no relation to evidence handling.

Regulatory compliance: Refers to adherence to laws and regulations, not evidence tracking.

Incident documentation: Details the incident but does not specifically track evidence handling.

CompTIA A+ 220-1102 Exam Objectives, Section 4.6: Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

Legal documentation and evidence handling procedures.

---

## **Question: 103**

---

A technician needs to configure a computer for a user to work from home so the user can still securely access the user's shared files and corporate email. Which of the following tools would best accomplish this task?

- A . MSRA
- B . FTP
- C . RMM
- D . VPN

---

**Answer: D**

---

Explanation:

To securely access shared files and corporate email from home, the best tool to use is a Virtual Private Network (VPN). Here's why:

**VPN (Virtual Private Network):** A VPN creates a secure connection over the internet, allowing the user to access the corporate network as if they were on-site. It encrypts the data transmitted between the user's home and the corporate network, ensuring privacy and security.

**MSRA (Microsoft Remote Assistance):** Used for remote support but not for accessing shared files and emails securely.

**FTP (File Transfer Protocol):** Used for transferring files but does not provide secure access to a corporate network or email.

**RMM (Remote Monitoring and Management):** Used by IT professionals to manage client systems remotely but not for user access to shared files and emails.

CompTIA A+ 220-1102 Exam Objectives, Section 2.9: Given a scenario configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

VPN configuration and security documentation.

---

### **Question: 104**

---

A user's home system has been infected with malware. A technician has isolated the system from the network and disabled System Restore. Which of the following should the technician do next?

- A . Perform an antivirus scan.
- B . Run Windows updates.
- C . Reimage the system.
- D . Enable System Restore.

---

### **Answer: A**

---

Explanation:

When dealing with a malware-infected system, isolating the system from the network and disabling System Restore are critical initial steps. The next step in the malware removal process should be:

**Perform an antivirus scan:** This helps to identify and remove the malware from the system. Running a thorough scan using updated antivirus software is essential to detect and clean any malicious files.

**Run Windows updates:** This is important for system security but should be done after the malware is removed to avoid further issues.

**Reimage the system:** This is a more drastic measure and should be considered if the antivirus scan cannot fully clean the system.

**Enable System Restore:** This should only be done after the system is confirmed to be clean.

CompTIA A+ 220-1102 Exam Objectives, Section 3.3: Given a scenario use best practice procedures for malware removal.

---

### Question: 105

---

A user receives a message on a PC stating it has been infected by malware. A technician runs a full scan on the user's machine and detects no malware. Later that day, the same message reappears. Which of the following steps should the technician take to restore the system to regular functionality?

- A . Check for Windows updates.
- B . Reimage the computer.
- C . Enable Windows Firewall.
- D . Run System File Checker.

---

**Answer: B**

---

Explanation:

In change management, the scope of a project lists all the changes that are taking place. The scope ensures that all team members understand the boundaries and extent of the project, helping to prevent unexpected changes. Here's a detailed explanation:

Scope: Defines the project's boundaries and deliverables, including all the planned changes. It ensures that everyone involved understands what is included and excluded in the project, minimizing unexpected changes.

Risk analysis: Identifies potential risks and their impact but does not list the changes.

Rollback plan: Provides a strategy for reverting changes if something goes wrong but does not list changes.

Review: Involves evaluating changes but does not compile the list of changes.

CompTIA A+ 220-1102 Exam Objectives, Section 4.2: Explain basic change-management best practices.

Change management documentation.

---

### Question: 106

---

Which of the following change management practices lists all the changes that are taking place for a project to ensure that no unexpected changes happen?

- A . Risk analysis
- B . Scope
- C . Rollback plan
- D . Review

---

**Answer: B**

---

Explanation:

In change management, the scope of a project lists all the changes that are taking place. The scope ensures that all team members understand the boundaries and extent of the project, helping to prevent unexpected changes. Here's a detailed explanation:

**Scope:** Defines the project's boundaries and deliverables, including all the planned changes. It ensures that everyone involved understands what is included and excluded in the project, minimizing unexpected changes.

**Risk analysis:** Identifies potential risks and their impact but does not list the changes.

**Rollback plan:** Provides a strategy for reverting changes if something goes wrong but does not list changes.

**Review:** Involves evaluating changes but does not compile the list of changes.

CompTIA A+ 220-1102 Exam Objectives, Section 4.2: Explain basic change-management best practices.

Change management documentation.

---

### **Question: 107**

---

A user identified that a program installed in a workstation does not have optional features enabled. Which of the following must the technician do to install the optional features?

- A . Go to Programs and Features, uninstall the program, and reinstall it.
- B . Go to Administrative Tools and edit System Configuration.
- C . Go to Administrative Tools and run Disk Cleanup.
- D . Go to Programs and Features, select the program, and click on Change.

---

**Answer: D**

---

Explanation:

When a user needs to install optional features for a program that is already installed, the technician should:

**Go to Programs and Features:** Access this via the Control Panel.

**Select the program:** Find the installed program in the list.

**Click on Change:** The 'Change' option allows modifications to the installed program, such as adding or removing features, without completely uninstalling and reinstalling the program.

This method is the most efficient and avoids unnecessary reinstallation of the software, which could lead to data loss or require reconfiguration.

CompTIA A+ 220-1102 Exam Objectives, Section 1.4: Given a scenario use the appropriate Microsoft Windows 10 Control Panel utility.

Windows application management documentation.

---

## **Question: 108**

---

During a routine check, a systems administrator discovers that a user's PC is running slowly and CPU utilization is at 100%. Further investigation shows a large amount of resource usage. Which of the following is the most likely cause of the high resource usage?

- A . Firewall activities
- B . Botnet attack
- C . DDoS attack
- D . Keylogger attack

---

## **Answer: B**

---

Explanation:

When a system administrator discovers a user's PC running slowly with 100% CPU utilization, it often indicates that the system is being used for unauthorized purposes, such as being part of a botnet attack. Here's why:

**Botnet attack:** Botnets are networks of computers infected with malware and controlled by an attacker. These infected computers (bots) are often used to carry out tasks like sending spam or participating in Distributed Denial of Service (DDoS) attacks. The high CPU utilization and resource usage indicate that the computer might be performing tasks dictated by the botnet controller.

**Firewall activities:** While firewall activities can use some resources, they generally do not cause sustained high CPU utilization.

**DDoS attack:** DDoS attacks target external systems by overwhelming them with traffic. A system participating in a DDoS might have high network usage, but the primary symptom on the user's PC would be high network activity, not necessarily CPU usage.

**Keylogger attack:** Keyloggers record keystrokes and generally do not cause high CPU utilization. They are more stealthy and have minimal resource footprints.

CompTIA A+ 220-1102 Exam Objectives, Section 2.4: Explain common social-engineering attacks, threats, and vulnerabilities.

Security and malware documentation.

---

## **Question: 109**

---

Which of the following will automatically map network drives based on Group Policy configuration?

- A . Log-in scripts
- B . Access control lists
- C . Organizational units
- D . Folder redirection

---

## **Answer: A**

---

Explanation:

Network drives can be automatically mapped for users based on Group Policy configuration using log-in scripts. Here's how it works:

Log-in scripts: These are scripts executed when a user logs in to a domain. They can be configured through Group Policy in Active Directory to map network drives automatically. The scripts can use commands like net use to map drives.

Access control lists (ACLs): While ACLs control permissions for files and folders, they do not automatically map network drives.

Organizational units (OUs): OUs are used to organize users and computers in a directory structure but do not map drives.

Folder redirection: This redirects the path of a folder to a new location, typically on a network share, but it does not automatically map drives.

CompTIA A+ 220-1102 Exam Objectives, Section 1.6: Given a scenario configure Microsoft Windows networking features on a client/desktop.

Group Policy and login script documentation from Microsoft.

---

### Question: 110

---

A user's laptop is shutting down every time the laptop lid is closed, which is leading to frequent work interruptions. Which of the following should a help desk specialist do to remediate the issue?

- A . Configure the sleep settings.
- B . Disable hibernation.
- C . Edit the power plan.
- D . Turn on fast startup.

---

**Answer: C**

---

Explanation:

When a user's laptop shuts down every time the lid is closed, it typically means that the power settings are configured to put the laptop into a shutdown state when the lid is closed. To remediate this issue:

Edit the power plan: This involves changing the settings for what happens when the laptop lid is closed.

Go to Control Panel > Hardware and Sound > Power Options.

Click on 'Choose what closing the lid does.'

Change the settings for 'When I close the lid' to either 'Sleep' or 'Do nothing' instead of 'Shut down.'

Configure the sleep settings: While similar to editing the power plan, this option specifically adjusts the sleep settings rather than the overall power plan settings.

Disable hibernation: This is a less direct solution but could be considered if the laptop was set to hibernate and then experiencing issues.

Turn on fast startup: This setting affects how quickly the computer starts up from a shutdown, but it does not directly address the issue of what happens when the lid is closed.

CompTIA A+ 220-1102 Exam Objectives, Section 1.5: Given a scenario, use the appropriate Microsoft Windows settings.

Windows power management documentation.

---

### **Question: 111**

---

A user reports that a new, personally owned tablet will not connect to the corporate Wi-Fi network. The user is able to connect to the Wi-Fi network with other devices, and the tablet is running the latest software. Which of the following is the most likely cause of the issue?

- A . Incorrect encryption settings
- B . Blocked MAC address
- C . Outdated drivers
- D . Disabled location services

---

### **Answer: B**

---

Explanation:

When a user reports that a new, personally owned tablet will not connect to the corporate Wi-Fi network, but other devices can connect, and the tablet is running the latest software, the most likely cause of the issue is a blocked MAC address. Here's why:

MAC Filtering: Many corporate networks implement MAC address filtering as a security measure. This involves only allowing devices with specific MAC addresses to connect to the network. If the MAC address of the new tablet is not on the allowed list, it will be blocked from connecting.

Check Network Settings: To troubleshoot this, the network administrator can check the network's MAC filtering settings to see if the tablet's MAC address is blocked.

Add MAC Address: If the MAC address is blocked, adding the tablet's MAC address to the allowed list will resolve the issue.

Other options like incorrect encryption settings or outdated drivers are less likely because the user can connect with other devices and the tablet is running the latest software. Disabled location services do not affect Wi-Fi connectivity.

CompTIA A+ 220-1102 Exam Objectives, Section 2.6: Given a scenario configure basic mobile device network connectivity and application support.

---

### Question: 112

---

A user with a disability needs to be able to press the Ctrl+Alt+Del keyboard sequence one key at a time. Which of the following turns on this Ease of Access feature?

- A . Press the Shift key five times in a row.
- B . Press Ctrl+Alt+Esc simultaneously.
- C . Press Ctrl+Alt+Tab simultaneously.
- D . Press the Windows key+Tab.

---

**Answer: A**

---

Explanation:

The Ease of Access feature in Windows that allows a user to press keyboard shortcuts one key at a time is called 'Sticky Keys.' Sticky Keys is designed to assist users with disabilities who have difficulty pressing multiple keys simultaneously. To enable Sticky Keys:

Press the Shift key five times in a row: This is the quickest method to activate Sticky Keys. When you press the Shift key five times, a dialog box appears, asking if you want to turn on Sticky Keys. This method is widely documented as the default shortcut for enabling this feature.

Confirmation dialog: A confirmation dialog will appear asking if you want to turn on Sticky Keys. Click 'Yes' to enable it.

Control Panel or Settings: Alternatively, you can enable Sticky Keys through the Control Panel or the Settings app. Go to 'Ease of Access' settings, find the 'Keyboard' section, and turn on Sticky Keys from there.

CompTIA A+ 220-1102 Exam Objectives, Section 1.4: Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

Windows Ease of Access documentation.

---

### Question: 113

---

#### SIMULATION

You have been contacted through the help desk chat application. A user is setting up a replacement SOHO router. Assist the user with setting up the router.

#### INSTRUCTIONS

Select the most appropriate statement for each response. Click the send button after each response to continue the chat. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A . See the solution below in Explanation

**Answer: A**

Explanation:

To: Customer

 I just received a new router for the office, and I need help setting it up.

 I am happy to assist you today.

 I need to set up my basic security settings.

 Is this the first router in your office?

 No, it is a replacement. The last router broke.  
I am currently logged in and connected to the router's web page.

 The first thing you need to do is change the default password.

 Create a new password with an uppercase, a lowercase, and a special character.

 That is complete now, and the router is asking to reboot. Should I reboot to move on?

 Yes, reboot please.

 What is next?

 Do you know the name of the network you connected to before?

 Yes.

 Change the SSID to the previously used network name.

 Also, make sure to change your wireless password to the one previously used.



That is done. Thank you for your help.



You are welcome. Is there anything else I can help you with?



No, I am all set.

---

### Question: 114

---

A technician is an administrator on a messaging application for a private work group of mixed departments. One of the technician's colleagues discloses to the group that their employer recently suffered a major security breach and shared details about the breach to the group. Which of the following should the technician do first?

- A . Ignore the messages as all of the group members work for the same employer.
- B . Remove the colleague from the group and ask members to delete the messages.
- C . Message the colleague privately and ask the colleague to delete the messages immediately.
- D . Contact the supervisor and report the colleague with screen shots of the messages

---

**Answer: D**

---

Explanation:

In the case of a security breach disclosure, it's crucial to follow proper protocol to handle sensitive information responsibly:

Ignore the messages: Not appropriate as it disregards the potential impact and severity of the breach.

Remove the colleague and ask members to delete the messages: While it might limit the spread of the information, it doesn't address the breach reporting requirement.

Message the colleague privately: Might help in immediate removal of messages but does not follow the proper chain of command and reporting protocols.

Contact the supervisor: The correct action, as it ensures that the incident is handled by higher authorities who can take appropriate measures. Reporting with screenshots ensures that there is evidence of the disclosure.

---

### Question: 115

---

A company wants to reduce the negative ecological impacts of its business and has decided to hire an e-waste company to dispose of equipment. Which of the following should the e-waste company provide the business?

- A . Non-disclosure agreement
- B . Certification of destruction
- C . Low-level formatting

D . Shredding/drilling

---

**Answer: B**

---

Explanation:

When disposing of e-waste, it is important to ensure that the data on the equipment is securely destroyed and that the disposal process complies with environmental regulations.

Non-disclosure agreement: Relates to confidentiality, not disposal.

Certification of destruction: The correct document verifying that the equipment has been disposed of in accordance with regulations and standards, ensuring data is irretrievably destroyed.

Low-level formatting: A method to wipe data but does not guarantee compliance with e-waste disposal regulations.

Shredding/drilling: Physical destruction methods that might be used, but certification of destruction is the documentation needed.

---

### **Question: 116**

---

A user in a SOHO asks an off-site, remote technician to connect securely to the user's laptop. The technician is able to connect to the VPN but is unable to connect to the user's laptop. Which of the following settings should the technician review?

- A . Wireless protocol
- B . DHCP pool
- C . Content filtering
- D . Firewall

---

**Answer: D**

---

Explanation:

When a technician is unable to connect to a laptop over a VPN, one of the most common reasons is that the firewall settings on either the laptop or the network are blocking the connection.

Wireless protocol: Unrelated, as the technician is already connected to the VPN.

DHCP pool: Unlikely to be the issue, as it deals with IP address assignment.

Content filtering: Typically involves filtering web content, not affecting direct connections.

Firewall: The correct setting to review, as it may block the necessary ports or services required for remote access.

---

### **Question: 117**

---

A technician needs to track evidence for a forensic investigation on a Windows computer. Which of the following describes this process?

- A . Valid license
- B . Data retention requirements
- C . Material safety data sheet
- D . Chain of custody

---

**Answer: D**

---

Explanation:

In forensic investigations, maintaining the integrity of the evidence is crucial. The chain of custody is a process that ensures that evidence has been collected, preserved, and transferred in a manner that is legally defensible.

Valid license: Refers to software licensing, irrelevant in this context.

Data retention requirements: Policies for how long data should be kept, but not specifically related to tracking forensic evidence.

Material safety data sheet: Documentation for handling hazardous materials, not applicable here.

Chain of custody: The correct process for documenting the handling and transfer of evidence to maintain its integrity and admissibility in court.

---

### **Question: 118**

---

A Windows user wants a filesystem that protects confidential data from attackers who have physical access to the system. Which of the following should the user choose?

- A . ext
- B . APFS
- C . FAT
- D . EFS

---

**Answer: D**

---

Explanation:

EFS (Encrypting File System) is a feature of Windows that provides filesystem-level encryption. It is designed to encrypt files and folders to protect them from unauthorized access, even if an attacker has physical access to the computer.

ext: A filesystem type used primarily in Linux, without native encryption features for Windows.

APFS: Apple's filesystem, used in macOS and iOS.

FAT: A simple filesystem type with no encryption features.

EFS: The correct choice for a Windows user needing to encrypt data at the filesystem level to protect against unauthorized physical access.

---

### Question: 119

---

Which of the following operating systems uses the ext4 filesystem type?

- A . macOS
- B . iOS
- C . Linux
- D . Windows

---

**Answer: C**

---

Explanation:

The ext4 (fourth extended filesystem) is a journaling file system for Linux. It is widely used in many Linux distributions due to its performance, robustness, and advanced features like large file and volume support.

macOS: Uses filesystems like HFS+ or APFS.

iOS: Uses APFS (Apple File System).

Linux: Uses ext4 among other filesystems like ext3, XFS, Btrfs, etc.

Windows: Uses NTFS, FAT32, and exFAT, not ext4.

---

### Question: 120

---

An employee lost a smartphone and reported the loss to the help desk. The employee is concerned about the possibility of a breach of private data.

a. Which of the following is the best way for a technician to protect the data on the phone?

- A . Remote lock
- B . Remote wipe
- C . Remote access
- D . Remote encrypt

---

**Answer: B**

---

Explanation:

When a smartphone is lost, especially one that might contain sensitive or private data, the primary concern is to ensure that any data on the device cannot be accessed by unauthorized persons. Among the options provided:

Remote lock: This option will lock the device remotely, preventing access. However, it does not remove the data and might not be effective if the device is powered off or reset.

Remote wipe: This is the best option as it allows the technician to erase all data from the device remotely, ensuring that sensitive information is not accessible to anyone who finds or steals the device.

Remote access: This option would allow a technician to access the device remotely, but it would not directly prevent unauthorized access or data breaches.

Remote encrypt: Encrypting the device remotely might not be possible if the device is not accessible or turned on, and it does not remove existing data which could be at risk.

---

### **Question: 121**

---

Users report that they can log in to the web application during business hours, but none of the application's functions are working properly. Company policy does not allow for the server to be rebooted during business hours. Which of the following should a technician do to fix the web application and follow company policy?

- A . Restart services.
- B . Roll back Windows updates.
- C . Perform a Windows repair.
- D . Add RAM to the server.

---

### **Answer: A**

---

Explanation:

Restarting services can resolve issues with web applications without requiring a full server reboot, which aligns with the company policy.

Restart services: Likely to resolve issues with the web application by refreshing the necessary services.

Roll back Windows updates: Unnecessary if the issue is with the application services.

Perform a Windows repair: More disruptive and not typically needed for application service issues.

Add RAM to the server: Would require a reboot and is not immediately necessary for troubleshooting application issues.

---

### **Question: 122**

---

A technician is adding some Windows 10 workstations to the corporate domain. A script was able to add the majority of the workstations, but failed on a couple. Which of the following menus should the technician check in order to complete the task manually?

- A . User Accounts
- B . System Properties

- C . Windows Firewall
- D . Network and Sharing

---

**Answer: B**

---

Explanation:

To manually add a workstation to a domain, the technician needs to access the System Properties menu where domain settings are configured.

User Accounts: Manages user accounts but does not handle domain membership.

System Properties: The correct place to add or change domain membership settings.

Windows Firewall: Manages firewall settings but not domain membership.

Network and Sharing: Manages network connections and sharing but not domain settings.

---

### **Question: 123**

---

A user is unable to see transaction details on a website, and nothing happens when the user clicks the details button. Which of the following should the user do to fix this issue?

- A . Clear the browser cache.
- B . Disable the pop-up blocker.
- C . Configure private browsing.
- D . Verify valid certificates.

---

**Answer: B**

---

Explanation:

Pop-up blockers can sometimes prevent essential pop-up windows required by websites to display transaction details.

Clear the browser cache: Helps with loading issues but not specific to pop-ups.

Disable the pop-up blocker: The correct solution, as it allows the blocked pop-up to be displayed.

Configure private browsing: Prevents storing browsing data but does not affect pop-ups.

Verify valid certificates: Ensures secure connections but does not resolve pop-up issues.

---

### **Question: 124**

---

Employees at comptia.org are reporting getting an usual amount of emails from a coworker. A technician discovers the emails were sent from the following address:

john@cOmpnia.org

Which of the following social engineering attacks is this an example of?

- A . Whaling
- B . Insider threat
- C . Phishing
- D . Vishing
- E . Evil twin

---

**Answer: C**

---

Explanation:

Phishing involves tricking individuals into disclosing sensitive information or installing malware through deceptive emails.

Whaling: A specific type of phishing targeting high-profile individuals.

Insider threat: Malicious activities by someone within the organization.

Phishing: General deceptive emails to trick users into compromising information or installing malware.

Vishing: Voice phishing, conducted over the phone.

Evil twin: A rogue Wi-Fi access point mimicking a legitimate one to intercept data.

---

### **Question: 125**

---

Which of the following is the weakest wireless security protocol?

- A . WEP
- B . WPA2
- C . TKIP
- D . AES

---

**Answer: A**

---

Explanation:

WEP (Wired Equivalent Privacy) is known to be the weakest wireless security protocol due to its vulnerabilities and ease of being compromised.

WEP: The oldest and weakest protocol, susceptible to various attacks and easily cracked.

WPA2: Much stronger security with AES encryption, currently one of the most secure standards.

TKIP: Used with WPA, stronger than WEP but weaker than WPA2 with AES.

AES: Advanced Encryption Standard, used in WPA2 and known for strong security.

---

### **Question: 126**

---

A user's work PC has been the target of multiple phishing attacks. Which of the following is a way for the user to prevent further attacks?

- A . Enabling Windows Firewall
- B . Activating the email spam filter
- C . Using a secure VPN connection
- D . Running vulnerability scans on a schedule

---

**Answer: B**

---

Explanation:

Phishing attacks are typically delivered via email, so the most effective immediate measure is to filter out these malicious emails.

Enabling Windows Firewall: Helps protect against network threats but does not specifically address phishing emails.

Activating the email spam filter: Directly targets phishing attempts by filtering and blocking suspicious emails before they reach the user.

Using a secure VPN connection: Enhances secure communications but does not prevent phishing attacks.

Running vulnerability scans on a schedule: Identifies and mitigates vulnerabilities but does not address phishing emails directly.

---

### **Question: 127**

---

An administrator received a new shipment of mobile devices. Per company policy, all enterprise-issued devices must have two authentication methods, and the organization has already enforced the use of PIN codes as one method. Which of the following device features should the administrator enable?

- A . Smart card
- B . Biometrics
- C . Hard token
- D . One-time password

---

**Answer: B**

---

Explanation:

For securing mobile devices with two authentication methods, combining something the user knows (a PIN) with something the user is (biometrics) enhances security by implementing multi-factor authentication.

Smart card: Generally requires additional hardware and is not commonly used in mobile devices.

Biometrics: Uses unique biological traits such as fingerprints or facial recognition, providing a convenient and secure second method of authentication.

Hard token: Involves additional physical devices which might not be practical for mobile devices.

One-time password: Usually used for specific applications rather than as a general device authentication method.

---

### **Question: 128**

---

A home office user wants to ensure a PC is backed up and protected against local natural disasters and hardware failures. Which of the following would meet the user's requirements?

- A . Using an agent-based cloud backup solution
- B . Implementing a grandfather-father-son backup rotation
- C . Automating backups to a local network share
- D . Saving files manually to an external drive

---

**Answer: A**

---

Explanation:

For ensuring data protection against local natural disasters and hardware failures, the best approach is to use an off-site solution that provides redundancy and is resilient to local disruptions.

Using an agent-based cloud backup solution: This method involves backing up data to a remote cloud server, providing protection against local disasters like floods, fires, or hardware failures since the data is stored off-site and can be accessed from anywhere.

Implementing a grandfather-father-son backup rotation: While effective for managing local backups, this method typically involves physical media which could still be vulnerable to local disasters.

Automating backups to a local network share: This keeps the backups within the same physical location, making them susceptible to local disasters.

Saving files manually to an external drive: This method is prone to human error and doesn't provide automated or off-site protection.

---

### **Question: 129**

---

A technician needs to configure security settings on a Windows 10 workstation. Which of the following should the technician configure to limit password attempts?

- A . Account Lockout Policy
- B . User Access Control
- C . System Protection
- D . Firewall

---

**Answer: A**

---

Explanation:

Configuring the Account Lockout Policy in Windows 10 is the appropriate action to limit password attempts. This security setting determines the number of failed login attempts that will trigger a lockout, preventing unauthorized access due to repeated password guessing. It is an effective measure to enhance security by deterring brute-force attacks.

---

### **Question: 130**

---

Which of the following macOS file types requires mounting before installation?

- A . .pkg
- B . .zip
- C . .app
- D . .dmg

---

**Answer: D**

---

Explanation:

The .dmg file type in macOS requires mounting before installation. .dmg files are disk image files used to distribute software on macOS. When opened, they mount a virtual disk on the desktop, from which the application can be installed. Other file types like .pkg, .zip, and .app have different processes for installation and do not require mounting in the same way.

---

### **Question: 131**

---

A web developer installs and launches a new external web server. Immediately following the launch, the performance of all traffic traversing the firewall degrades substantially. Which of the following considerations was overlooked?

- A . OS compatibility
- B . Quality of service
- C . 32- vs. 64-bit architecture
- D . Storage requirements

---

**Answer: B**

---

## Explanation:

The performance degradation following the launch of a new external web server suggests that Quality of Service (QoS) considerations were overlooked. QoS settings help prioritize traffic to ensure that critical services like web servers receive the bandwidth they need without negatively impacting the overall network performance. Without proper QoS configuration, the new server's traffic could overwhelm the firewall, leading to widespread performance issues.

---

### Question: 132

---

A user's workstation was infected with a newly discovered virus that the AV system detected. After a full virus scan and a workstation reboot, the virus is still present in the OS. Which of the following actions should the user take to remove the virus?

- A . Enable the system firewall.
- B . Use bootable antivirus media to scan the system.
- C . Download software designed to specifically target the virus.
- D . Run the operating system update process.

---

### Answer: B

---

## Explanation:

Using bootable antivirus media to scan the system is an effective method for removing a persistent virus. Booting from external antivirus media allows the system to scan for and remove malware without the infected operating system running, which can prevent the virus from hiding or resisting removal efforts that might occur within the active OS environment.

---

### Question: 133

---

A technician wants to update the local security policies on a Windows machine but is unable to launch the expected snap-in. Which of the following is the most likely reason?

- A . The computer is running Windows Home.
- B . The user did not sign the end user license agreement.
- C . The user disabled the User Account Control.
- D . An antivirus application is blocking access.

---

### Answer: A

---

## Explanation:

The inability to launch the expected security policy snap-in is likely because the computer is running Windows Home edition, which does not include the Group Policy Editor or certain other administrative tools available in Professional,

Enterprise, and Education editions. The Home edition is designed for general consumer use and lacks some of the advanced security and management features found in higher editions.

---

### Question: 134

---

A Windows 10 computer is not installing updates and continues to receive errors even during manual update installations. Which of the following should a technician do to fix the issues? (Select two).

- A . Ensure that the Windows Update Utility is the latest version.
- B . Refresh local WSUS settings on the computer.
- C . Delete the Windows Update cache.
- D . Run the System check to verify system files.
- E . Reimage the operating system while retaining user files.
- F . Reset WMI and re-register system .dlls.

---

**Answer: B, C**

---

Explanation:

Refreshing local Windows Server Update Services (WSUS) settings and deleting the Windows Update cache are effective steps in resolving issues with Windows 10 not installing updates. These actions help in rectifying any corrupt update files and ensuring that the workstation is properly communicating with the update servers, which can resolve errors during manual and automatic update installations.

---

### Question: 135

---

A company uses shared drives as part of a workforce collaboration process. To ensure the correct access permissions, inheritance at the top-level folder is assigned to each department. A manager's team is working on confidential material and wants to ensure only the immediate team can view a specific folder and its subsequent files and subfolders. Which of the following actions should the technician most likely take?

- A . Turn off inheritance on the requested folder only and set the requested permissions to each file manually.
- B . Turn off inheritance at the top-level folder and remove all inherited permissions.
- C . Turn off inheritance at the top-level folder and set permissions to each file and subfolder manually.
- D . Turn off inheritance on the requested folder only, set the requested permissions, and then turn on inheritance under the child folders.

---

**Answer: D**

---

Explanation:

Turning off inheritance on the specific folder requested by the manager and setting the requested permissions, followed by turning on inheritance under the child folders, ensures that only the immediate team has access to the confidential material while maintaining the broader permissions structure for other folders and files. This action

isolates the folder's permissions from the top-level inheritance, providing a focused security measure for sensitive content.

---

### Question: 136

---

A customer service representative is unable to send jobs to a printer at a remote branch office. However, the representative can print successfully to a local network printer. Which of the following commands should a technician use to view the path of the network traffic from the PC?

- A . netstat
- B . ping
- C . format
- D . tracert

---

**Answer: D**

---

Explanation:

The 'tracert' command is used to view the path that network traffic takes from a PC to a specified destination. It is helpful in identifying where along the path the traffic may be failing or experiencing delays. In the scenario where a customer service representative can't send jobs to a remote printer but can print locally, 'tracert' can help diagnose if there's a network routing issue affecting the connection to the remote branch office.

---

### Question: 137

---

A technician is installing software on a user's workstation. The installation fails due to incompliance with the HCL. Which of the following components is most likely causing the installation to fail? (Select two).

- A . NIC
- B . CPU
- C . PSU
- D . KVM
- E . RAM
- F . DVI

---

**Answer: A, B**

---

Explanation:

The Hardware Compatibility List (HCL) is a list that indicates hardware components that are compatible with a specific software or operating system. If software installation fails due to incompliance with the HCL, it's most likely due to core hardware components like the Network Interface Card (NIC) or the Central Processing Unit (CPU) not being supported or not meeting the software's minimum hardware requirements. The PSU, KVM, RAM, and DVI are less likely to directly impact software compatibility as defined by the HCL.

---

### **Question: 138**

---

A user reports that an Android mobile device takes a long time to boot, and all applications crash when launched. The user installed the applications from a third-party website. Which of the following steps should the technician complete to diagnose the issue?

- A . Scan the system for malware.
- B . Clear the web browser cache.
- C . Enroll the device in an MDM system.
- D . Confirm the compatibility of the applications with the OS.

---

**Answer: A**

---

Explanation:

When an Android device experiences slow boot times and application crashes after installing apps from a third-party website, scanning the system for malware is a critical first step. Third-party sources can often host malicious software that can compromise device performance and security. A malware scan can identify and remove such threats, potentially resolving the performance issues and application instability. Clearing the web browser cache, enrolling the device in an MDM system, and confirming app compatibility are useful steps but do not address the immediate concern of potential malware introduced by third-party app installations.

---

### **Question: 139**

---

Which of the following features can be used to ensure a user can access multiple versions of files?

- A . Multiple desktops
- B . Remote Disc
- C . Time Machine
- D . FileVault

---

**Answer: C**

---

Explanation:

Time Machine is a backup feature available in macOS that automatically makes hourly backups for the past 24 hours, daily backups for the past month, and weekly backups for all previous months to an external drive or NAS. It allows users to recover the entire system or specific files from any point in time, ensuring access to multiple versions of files. This feature is particularly useful for reverting to earlier versions of a document or recovering a file that has been accidentally deleted or altered. The other options, such as Multiple Desktops, Remote Disc, and FileVault, do not provide versioning capabilities for file access.

---

### **Question: 140**

---

A user is unable to start a computer following a failed Windows 10 update. When trying to start the computer, the user sees a blue screen of death. Which of the following steps should a technician take to diagnose the issue?

- A . Perform a safe mode boot.
- B . Run the System Restore wizard.
- C . Start the computer in the last known-good configuration.
- D . Reset the BIOS settings.

---

**Answer: A**

---

Explanation:

Booting in safe mode is the initial step to diagnose a computer experiencing a blue screen of death (BSOD) following a failed Windows 10 update. Safe mode starts the computer with a minimal set of drivers and services, allowing troubleshooting and identification of the problematic software or driver causing the BSOD. This mode provides a safer environment to uninstall recent updates or drivers, perform system scans, and restore the system if necessary. Other options like System Restore wizard, last known-good configuration, and resetting BIOS settings may be subsequent steps but do not directly diagnose the issue as effectively as booting in safe mode.

---

### **Question: 141**

---

Multiple users routinely record log-in information in readily accessible areas. Which of the following is the best way to mitigate this issue?

- A . Trusted sources
- B . Valid certificates
- C . User training
- D . Password manager

---

**Answer: D**

---

Explanation:

Using a password manager is the best way to mitigate the issue of users recording their login information in accessible areas. Password managers securely store and encrypt passwords and login details, reducing the need for users to write down or remember multiple complex passwords. This approach enhances security by encouraging the use of strong, unique passwords for different accounts without the risk of forgetting them or the unsafe practice of writing them down. Trusted sources, valid certificates, and user training are important security measures but do not directly address the problem of managing multiple secure passwords as effectively as a password manager does.

---

### **Question: 142**

---

An administrator needs to back up the following components of a single workstation:

- \* The installation of the operating system
- \* Applications
- \* User profiles
- \* System settings

Which of the following backup methods can the administrator use to ensure the workstation is properly backed up?

- A . Differential
- B . Image
- C . Synthetic
- D . Archive

---

**Answer: B**

---

Explanation:

An image backup captures a complete snapshot of the entire system at a specific point in time, including the operating system, installed applications, user profiles, and system settings. This method is most suitable for backing up the components listed in the question because it ensures that every aspect of the workstation, from the core OS to individual user settings, is preserved and can be restored in its entirety. This is crucial for quickly recovering a system to a fully operational state after a failure or when migrating to new hardware. Other methods like differential, synthetic, and archive backups do not provide the comprehensive one-step restoration capability that an image backup offers for the complete system recovery.

---

### **Question: 143**

---

A user received an alert from a Windows computer indicating low storage space. Which of the following will best resolve this issue?

- A . Reviewing System Information
- B . Running Disk Cleanup
- C . Editing the Registry
- D . Checking the Performance Monitor
- E . Increasing the memory

---

**Answer: B**

---

---

### **Question: 144**

---

A company was recently attacked by ransomware. The IT department has remediated the threat and determined that the attack method used was email. Which of the following is the most effective way to prevent this issue from reoccurring?

- A . Spam filtering

- B . Malware prevention software
- C . End user education
- D . Stateful firewall inspection

---

**Answer: C**

---

Explanation:

To prevent ransomware attacks via email, the most effective way is End user education (C). Educating users about the dangers of phishing emails, how to recognize suspicious emails, and the importance of not clicking on unknown links or attachments can significantly reduce the risk of ransomware infections. Awareness and training can empower users to act as the first line of defense against such cyber threats

---

### **Question: 145**

---

A technician is troubleshooting a Windows 10 PC that has experienced a BSOD. The user recently installed optional Windows updates. Which of the following is best way to resolve the issue?

- A . Enable System Restore.
- B . Roll back the device drivers.
- C . Reinstall the OS.
- D . Update the BIOS.

---

**Answer: B**

---

Explanation:

To resolve a BSOD issue on a Windows 10 PC after installing optional Windows updates, the best approach is to Roll back the device drivers (B). BSODs can often be caused by incompatible or faulty drivers introduced during an update. Rolling back the drivers to a previous version can restore system stability and resolve the BSOD issue.

---

### **Question: 146**

---

A technician is following the ticketing system's best practices when handling user support requests. Which of the following should the technician do first when responding to a user support request that contains insufficient information?

- A . Ask the user for clarification.
- B . Keep the user updated on the progress.
- C . Document the root cause.
- D . Follow the system's escalation process.

---

**Answer: A**

---

**Explanation:**

When handling a user support request that contains insufficient information, the first step a technician should take is to Ask the user for clarification (A). This involves gathering more details about the issue to understand the problem better and provide an accurate resolution. Effective communication and asking the right questions are essential for diagnosing and resolving IT issues efficiently.

---

### **Question: 147**

---

Which of the following languages is used for scripting the creation of Active Directory accounts?

- A . Bash
- B . Structured Query Language
- C . Hypertext Preprocessor
- D . PowerShell

---

**Answer: D**

---

**Explanation:**

For scripting the creation of Active Directory accounts, PowerShell (D) is used. PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language. It is built on the .NET framework and is particularly suited for automating and managing Windows-based systems, including Active Directory tasks.

---

### **Question: 148**

---

An employee has been using the same password for multiple applications and websites for the past several years. Which of the following would be best to prevent security issues?

- A . Configuring firewall settings
- B . Implementing expiration policies
- C . Defining complexity requirements
- D . Updating antivirus definitions

---

**Answer: B**

---

**Explanation:**

To prevent security issues related to an employee using the same password for multiple applications and websites, implementing expiration policies (B) is best. Password expiration policies require users to change their passwords at regular intervals, which helps to mitigate the risks associated with password reuse. Regularly changing passwords reduces the chances of unauthorized access from compromised credentials.

---

### **Question: 149**

---

Which of the following environmental controls is most important to maintain the safety of a data center?

- A . Temperature control
- B . Humidity control
- C . Fire suppression control
- D . Power management control

---

**Answer: A**

---

Explanation:

The most important environmental control to maintain the safety of a data center is Temperature control (A). Proper temperature control is crucial to prevent overheating, which can lead to hardware failure, reduced performance, and shortened equipment lifespan. Data centers house high-density computing equipment that generates significant amounts of heat, making effective temperature management essential for maintaining operational stability and reliability.

---

### **Question: 150**

---

Which of the following operating systems was the app file type designed to run under as an application file bundle?

- A . macOS
- B . Chrome
- C . Windows
- D . Linux

---

**Answer: A**

---

Explanation:

The app file type is designed to run under macOS as an application file bundle. macOS uses application bundles to store executable files and related resources, such as libraries, image files, and localized content, in a single directory hierarchy. This approach simplifies application management and execution within the macOS environment.

---

### **Question: 151**

---

A user's company phone has several pending software updates. A technician completes the following steps:

- \* Rebooted the phone
- \* Connected to Wi-Fi
- \* Disabled metered data

Which of the following should the technician do next?

- A . Restore the factory settings.
- B . Clean the browser history.
- C . Uninstall and reinstall the applications.
- D . Clear the cache.

---

**Answer: D**

---

Explanation:

After rebooting the phone, connecting to Wi-Fi, and disabling metered data, the next step the technician should take is to Clear the cache (D). Clearing the cache can resolve issues with the phone's performance and is often necessary before updating software to ensure that the updates can be downloaded and installed without issues. It removes temporary files that may be interfering with the update process.

---

### **Question: 152**

---

A network administrator wants to enforce a company's security policy that prohibits USB drives on user workstations. Which of the following commands should the administrator run on the users' workstations?

- A . diskpart
- B . chown
- C . gpupdate
- D . netstat

---

**Answer: C**

---

Explanation:

To enforce a security policy that prohibits USB drives on user workstations, the network administrator should run the gpupdate (C) command. This command forces a Group Policy update, which can include policies to disable USB drives. Group Policy is a feature in Microsoft Windows that allows for centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.

---

### **Question: 153**

---

A technician is upgrading the Microsoft Windows 10 OS. Which of the following are required for the technician to safely upgrade the OS? (Select two).

- A . Release notes
- B . Antivirus software
- C . Backup of critical data
- D . Device drivers
- E . Word processing software

F . Safe boot mode

---

**Answer: C, D**

---

Explanation:

To safely upgrade the Microsoft Windows 10 OS, it is essential to backup critical data (C) and ensure that you have the necessary device drivers (D). Backing up critical data protects against potential data loss during the upgrade process. Having the correct device drivers ensures that the hardware components function properly with the new OS version, preventing issues like loss of functionality or compatibility problems.

---

### **Question: 154**

---

Which of the following operating systems were designed for smartphones? (Select two).

- A . Ubuntu
- B . CentOS
- C . macOS
- D . Chrome OS
- E . iOS
- F . Android

---

**Answer: E, F**

---

Explanation:

The operating systems designed for smartphones include iOS and Android. iOS is developed by Apple Inc. for its iPhone range, while Android, developed by Google, is used across a variety of devices from different manufacturers. Both operating systems are specifically tailored to provide a mobile computing experience, with interfaces, applications, and functionalities designed for touchscreen input and mobile hardware.

---

### **Question: 155**

---

A user submits a request to have a graphics application installed on a desktop. When the technician attempts to install the application, the installation fails and the error message 'Not compatible with OS' is displayed. Which of the following is the most likely reason for this error message?

- A . The graphics card driver needs to be updated
- B . The application installer is 64-bit.
- C . The installation requires administrative rights.
- D . The disk space is inadequate.

---

**Answer: C**

---

## Explanation:

The most likely reason for an error message stating 'Not compatible with OS' during a software installation is that the installation requires administrative rights. Many software installations, especially those that affect system files or install drivers, require administrative privileges to execute correctly. Without these rights, the installer cannot make the necessary changes to the system, leading to such error messages.

---

### Question: 156

---

A user clicked a link in an email, and now the cursor is moving around on its own. A technician notices that File Explorer is open and data is being copied from the local drive to an unknown cloud storage location. Which of the following should the technician do first?

- A . Investigate the reported symptoms.
- B . Run anti-malware software.
- C . Educate the user about dangerous links.
- D . Quarantine the workstation.

---

**Answer: D**

---

---

### Question: 157

---

A network administrator is setting up the security for a SOHO wireless network. Which of the following options should the administrator enable to secure the network?

- A . NAT
- B . WPA3
- C . 802.1X
- D . Static IP

---

**Answer: B**

---

## Explanation:

To secure a SOHO wireless network, enabling WPA3 is the recommended option. WPA3 (Wi-Fi Protected Access 3) is the latest security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. It provides cutting-edge security protocols and cryptographic methods to enhance and replace its predecessors, WPA2 and WPA, offering improved protection against brute-force attacks and ensuring better privacy on public networks.

---

### Question: 158

---

A user's Windows desktop has low disk space. A technician thinks some upgrade files were never removed. Which of the following tools should the technician use to correct the issue?

- A . devmgmt.msc
- B . cleanmgr.exe
- C . dfrgui.exe
- D . diskmgmt.mac

---

**Answer: B**

---

Explanation:

The correct tool to use for removing upgrade files and freeing up disk space on a Windows desktop is cleanmgr.exe, which stands for Disk Cleanup. Disk Cleanup is a maintenance utility included in Microsoft Windows designed to free up disk space on a computer's hard drive. The utility scans and analyzes the hard drive for files that are no longer of any use, and then removes the unnecessary files. It can delete temporary files, system files, empty the Recycle Bin, and remove a variety of system files and other items that you might no longer need.

---

### **Question: 159**

---

A technician needs to implement a system to handle both authentication and authorization. Which of the following meets this requirement?

- A . WPA3
- B . MFA
- C . TACACS+
- D . RADIUS

---

**Answer: C**

---

Explanation:

To implement a system that handles both authentication and authorization, TACACS+ (Terminal Access Controller Access-Control System Plus) is the best option. TACACS+ is a security protocol that provides centralized Authentication, Authorization, and Accounting (AAA) services for networked access control, meeting the requirement for both authentication and authorization management.

---

### **Question: 160**

---

A technician needs to update the software on several hundred Mac laptops. Which of the following is the best method to complete the task?

- A . SSH
- B . MDM
- C . RDP
- D . SFTP

---

**Answer: B**

---

Explanation:

For updating software on several hundred Mac laptops, the best method is Mobile Device Management (MDM). MDM solutions allow administrators to remotely manage and update software across multiple devices efficiently, making it an ideal choice for handling software updates on a large scale.

---

### **Question: 161**

---

A technician needs to troubleshoot a user's computer while the user is connected to the system. The technician must also connect to the user's system using remote access tools built in to Windows. Which of the following is the best option to troubleshoot the user's computer?

- A . Screen share
- B . MSRA
- C . Virtual network computer
- D . RDP

---

**Answer: B**

---

Explanation:

To troubleshoot a user's computer remotely while the user is connected, the best option is Microsoft Remote Assistance (MSRA). MSRA allows the technician to view and control the user's screen with their permission, facilitating an effective troubleshooting session without disconnecting the user.

---

### **Question: 162**

---

A technician downloaded an OS installation file but is unable to run it. When the technician tries to open the file, a message indicates no software is installed to run this file. Which of the following should the technician do next to attempt to access the OS file?

- A . Request physical media
- B . Mount the ISO file.
- C . Install a third-party software.
- D . Download an appropriate 32-bit/64-bit OS file.

---

**Answer: B**

---

Explanation:

If a technician is unable to run an OS installation file and receives a message indicating no software is installed to handle the file, the next step is to mount the ISO file. Mounting the ISO will create a virtual drive from which the installation can be run, mimicking the behavior of a physical installation media.

---

### **Question: 163**

---

While browsing the internet, a customer sees a window stating antivirus protection is no longer functioning. Which of the following steps should a technician take next? (Select two).

- A . Isolate the computer from the network
- B . Enable the firewall service.
- C . Update the endpoint protection software
- D . Use System Restore to undo changes.
- E . Delete the browser cookies
- F . Run sfc /scannow.

---

**Answer: A**

---

Explanation:

When encountering a warning about antivirus protection malfunctioning, the first step should be to isolate the computer from the network to prevent potential spread of malware. Updating the endpoint protection software is also crucial to ensure the latest virus definitions and security features are in place to effectively identify and remove the threat.

---

### **Question: 164**

---

Which of the following best describes a rollback plan?

- A . A developer configures a process to return to the starting state upon completion.
- B . A user asks to remove an unneeded fileshare.
- C . An administrator applies new settings to a computer after the previous settings failed.
- D . A technician reverts the system to a previous state following a failed upgrade.

---

**Answer: D**

---

Explanation:

A rollback plan describes the process of reverting a system to its previous state after a failed upgrade or change. This ensures system stability and functionality by restoring known good configurations and is a crucial part of change management to minimize disruptions in case of unsuccessful updates.

---

### **Question: 165**

---

A user opened an infected email. A security administrator responded to the malicious event, successfully mitigated the situation, and returned the machine to service. Which of the following needs to be completed before this event is considered closed?

- A . Acceptable use policy
- B . Incident report
- C . End user license agreement
- D . Standard operating procedures

---

**Answer: B**

---

Explanation:

After successfully mitigating a malicious event caused by an infected email, the final step before considering the event closed is to complete an incident report. This document should detail the nature of the incident, the steps taken to resolve it, and any lessons learned to improve future responses to similar threats.

---

### **Question: 166**

---

A technician wants to harden Windows workstations after a recent security audit indicated the company is vulnerable to brute-force attacks. Which of the following features should the technician implement to mitigate such attacks?

- A . System screen lock
- B . Failed log-in lockout
- C . Restricted user permissions
- D . Data-at-rest encryption

---

**Answer: B**

---

Explanation:

To mitigate brute-force attacks, implementing a failed log-in lockout feature is effective. This security measure temporarily disables user accounts after a specified number of unsuccessful login attempts, preventing attackers from continuously trying different password combinations to gain unauthorized access.

---

### **Question: 167**

---

A technician is setting up a new PC in a SOHO. Which of the following should the technician most likely configure on the PC?

- A . VDI
- B . Mapped drives

C . Wireless WAN

D . Domain

---

**Answer: B**

---

Explanation:

In a Small Office/Home Office (SOHO) setup, the technician is most likely to configure mapped drives on a new PC. Mapped drives allow for easy access to shared resources such as files and printers on the network. This setup facilitates file sharing and collaboration within a small network, making it an essential configuration for SOHO environments.

---

### **Question: 168**

---

A technician is troubleshooting a user's PC that is running slowly and displaying frequent pop-ups. The technician thinks malware may be causing the issues, but before the issues began the user installed anti-malware software in response to a pop-up window. Which of the following is the most likely cause of these issues'?

- A . Expired certificate
- B . False alert
- C . Missing system files
- D . OS update failure

---

**Answer: B**

---

Explanation:

The scenario described is characteristic of a malware tactic known as scareware, where users are tricked into installing malware through false alerts claiming that their system is infected. The anti-malware software installed in response to a pop-up is likely malicious, causing the system to run slowly and display frequent pop-ups.

---

### **Question: 169**

---

Which of the following language types enables the automation of tasks?

- A . Compiled
- B . Scripting
- C . Web
- D . Database

---

**Answer: B**

---

Explanation:

Scripting languages are designed for automating tasks by writing scripts that can execute a series of commands. They are typically easier to write and understand compared to compiled languages and are widely used for automating repetitive tasks, making them the best option for task automation.

---

### **Question: 170**

---

A technician needs to configure a computer for a user to work from home so the user can still securely access the user's shared files and corporate email. Which of the following tools would best accomplish this task\*?

- A . MSRA
- B . FTP
- C . RMM
- D . VPN

---

**Answer: D**

---

Explanation:

A Virtual Private Network (VPN) creates a secure connection over the internet to a network, allowing a user to access shared files and corporate email as if they were directly connected to the network. This makes VPN the best tool for secure remote work access, compared to the other options which do not offer the same level of secure, remote network access.

---

### **Question: 171**

---

A technician is troubleshooting a user's PC that is displaying pop-up windows, which are advertising free software downloads. When the technician tries to open a document, the system displays an error message that reads: Not enough memory to perform this operation. Which of the following should be the technician's next step to resolve this issue?

- A . Install antispyware
- B . Reimage the system
- C . Disable the pop-up blocker
- D . Upgrade the browser
- E . Install antivirus software

---

**Answer: A**

---

Explanation:

The presence of pop-up windows advertising free software and the error message about memory are indicative of spyware infection. Installing and running antispyware software is a practical first step to remove the unwanted software and resolve the issue without resorting to more drastic measures like re-imaging the system.

---

## **Question: 172**

---

Which of the following features can a technician use to ensure users are following password length requirements?

- A . Group Policy
- B . Log-on script
- C . Access control list
- D . Security groups

---

**Answer: A**

---

Explanation:

Group Policy is a feature in Windows that allows network administrators to manage and configure operating system, application settings, and user settings in an Active Directory environment. It can enforce password policies across the network, including password length requirements, making it the best tool for ensuring compliance with security policies.

---

## **Question: 173**

---

An employee using an Apple MacBook is receiving frequent, random pop-up requests from other Apple devices wanting to share photos and videos and asking whether the user would like to accept the request. Which of the following configurations should the technician advise the user to change first?

- A . Wi-Fi
- B . iCloud
- C . Antivirus
- D . AirDrop

---

**Answer: D**

---

---

## **Question: 174**

---

Which of the following commands lists running processes in Linux?

- A . top
- B . apt-get
- C . ls
- D . cat

---

**Answer: A**

---

Explanation:

The 'top' command in Linux is used to display the running processes along with information about system resources like CPU and memory usage. It provides a real-time view of the system's resource consumption, making it an essential tool for monitoring and managing system performance.

---

### Question: 175

---

A user accidentally installed the incorrect word processing application on an iMac. Which of the following would allow the user to uninstall the incorrect application?

- A . Move the application to the desktop and press delete
- B . Identify the application in Finder and drag it to the trash can.
- C . Use Spotlight to search for the application, and then run the application.
- D . Use Time Machine to go back to the date before the installation.

---

### Answer: B

---

Explanation:

On macOS, uninstalling an application typically involves locating the app in Finder and dragging it to the Trash. This method is straightforward and commonly used for removing unwanted applications. The other options do not directly relate to the standard process of uninstalling applications on a Mac.

---

### Question: 176

---

A technician is installing a new copy of Windows on all computers in the enterprise Given the following requirements:

- \* The install phase must be scripted to run over the network
- \* Each computer requires a new SSD as the system drive,
- \* The existing HDD should remain as a backup drive.

Which of the following command-line tools should the technician use to install the drive and transfer the installation files from the network share? (Select three).

- A . net use
- B . robocopy
- C . winver
- D . diskpart
- E . sfc
- F . r.etstat
- G . ping
- H . chkdsk

---

### Answer: A, B, D

---

Explanation:

For scripted network installations requiring new SSDs and keeping HDDs as backup, the necessary tools are: 'net use' to connect to network shares, 'robocopy' to copy files efficiently from the network share to the local drive, and 'diskpart' to manage disk partitions, including initializing and formatting the new SSD. The other options are not relevant to the installation process as described.

---

### Question: 177

---

A customer wants to make sure the data is protected and secure on a Windows laptop's hard drive. Which of the following is the best solution?

- A . Windows Backup
- B . BitLocker
- C . Shadow Copy
- D . Trusted Platform Module

---

**Answer: B**

---

Explanation:

BitLocker is a full-disk encryption feature included with Windows Vista and later. It is designed to protect data by providing encryption for entire volumes. By encrypting the hard drive, BitLocker prevents unauthorized access to the data stored on the drive, securing it in case the laptop is lost or stolen. BitLocker is preferable over options like Windows Backup (which is for data recovery, not encryption), Shadow Copy (used for backup and does not encrypt data), and Trusted Platform Module (TPM, which is a hardware component used alongside BitLocker for securing encryption keys).

---

### Question: 178

---

#### SIMULATION

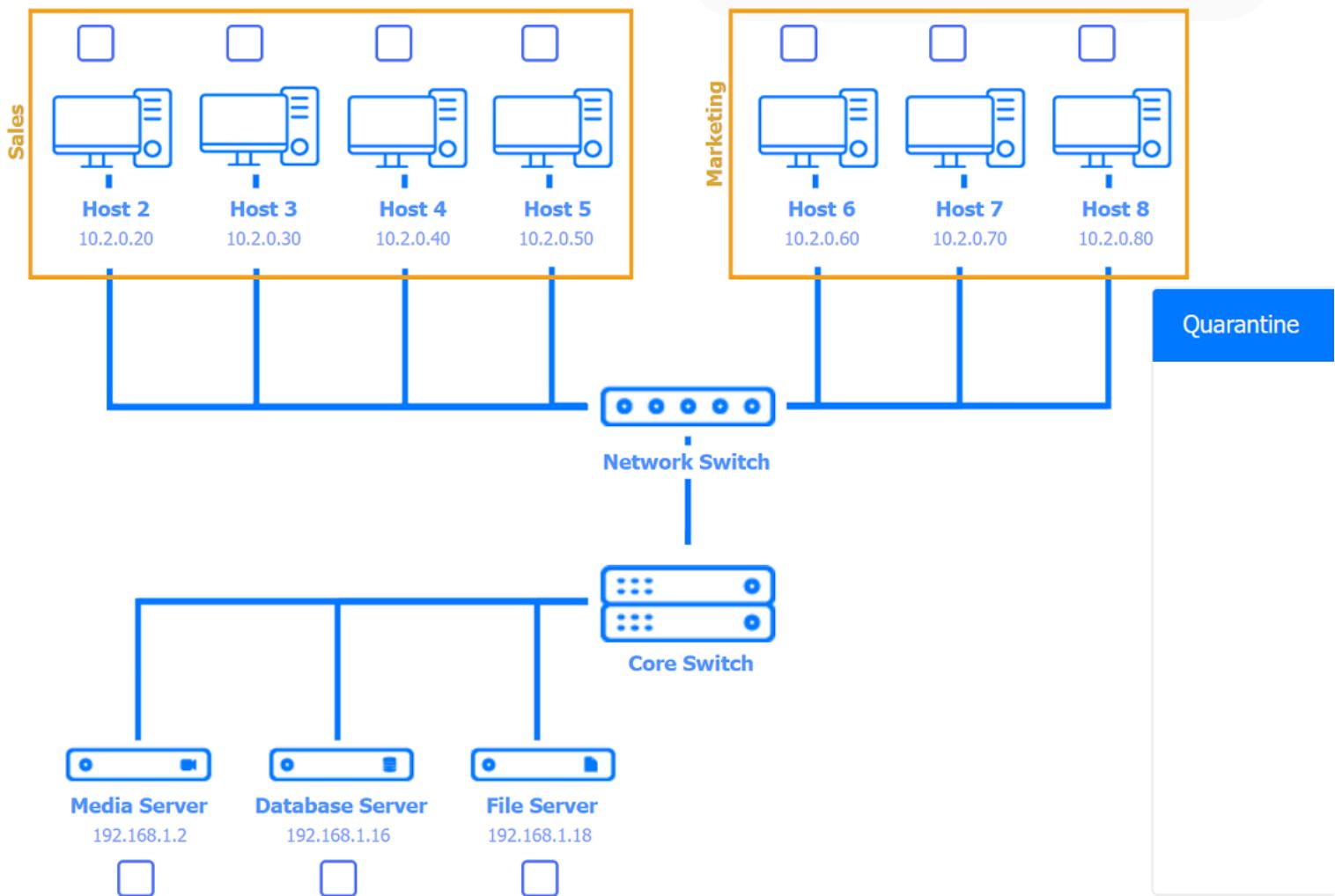
Multiple users are reporting audio issues as well as performance issues after downloading unauthorized software. You have been dispatched to identify and resolve any issues on the network using best practice procedures.

#### INSTRUCTIONS

Quarantine and configure the appropriate device(s) so that the users' audio issues are resolved using best practice procedures.

Multiple devices may be selected for quarantine.

Click on a host or server to configure services.



## Host 2 Services



Name	Status
Application Information	Started
Background Intelligent Transfer Service	Started
Bluetooth Support Service	Started
DHCP Client	Started
DNS Client	Started
Extensible Authentication Protocol	Started
Network Connections	Started
Netlogon	Started
Offline Files	Started
Parental Controls	Started
Persistance.j1zpxn Installer Service	Started

**Host 2 Services**

Name	Status
Volume Shadow Copy	▼
Windows Audio	▼
Windows Backup	▼
Windows CardSpace	▼
Windows Defender	▼
Windows Event Log	Started ▼
Windows Firewall	▼
Windows Installer	▼
Windows Search	Started ▼
Windows Time	▼
Windows Update	Started ▼

**Media Server Services**

Name	Status
Application Information	▼
Background Intelligent Transfer Service	Started ▼
Bluetooth Support Service	▼
DHCP Client	Started ▼
DNS Client	Started ▼
Extensible Authentication Protocol	Started ▼
Network Connections	Started ▼
Netlogon	▼
Offline Files	▼
Parental Controls	▼
Plug and Play	Started ▼

## Database Server Services



Name	Status
Application Information	<input type="button" value="▼"/>
Background Intelligent Transfer Service	<input type="button" value="Started ▼"/>
Bluetooth Support Service	<input type="button" value="▼"/>
DHCP Client	<input type="button" value="Started ▼"/>
DNS Client	<input type="button" value="Started ▼"/>
Extensible Authentication Protocol	<input type="button" value="Started ▼"/>
Network Connections	<input type="button" value="Started ▼"/>
Netlogon	<input type="button" value="▼"/>
Offline Files	<input type="button" value="▼"/>
Parental Controls	<input type="button" value="▼"/>
Plug and Play	<input type="button" value="Started ▼"/>

## File Server Services



Name	Status
Application Information	<input type="button" value="▼"/>
Background Intelligent Transfer Service	<input type="button" value="Started ▼"/>
Bluetooth Support Service	<input type="button" value="▼"/>
DHCP Client	<input type="button" value="Started ▼"/>
DNS Client	<input type="button" value="Started ▼"/>
Extensible Authentication Protocol	<input type="button" value="Started ▼"/>
Network Connections	<input type="button" value="Started ▼"/>
Netlogon	<input type="button" value="▼"/>
Offline Files	<input type="button" value="▼"/>
Parental Controls	<input type="button" value="▼"/>
Plug and Play	<input type="button" value="Started ▼"/>

A . See the Explanation for the solution

---

**Answer: A**

---

Explanation:

Host 2 and Media Server put them to Quarantine.

---

### Question: 179

---

A technician wants to improve password security after several users admitted to using very simple passwords. Which of the following is the best way to resolve this issue?

- A . Requiring four character types
- B . Decreasing the password expiration times
- C . Enabling an automatic lock timer
- D . Adding two characters to the minimum password length

---

**Answer: A**

---

Explanation:

Improving password security is crucial to protect user accounts from unauthorized access. Requiring passwords to include four character types---uppercase letters, lowercase letters, numbers, and special characters---significantly enhances password complexity. This diversity in characters makes passwords much harder to guess or crack using common methods like brute force attacks, thereby improving overall security.

Requiring four character types: This approach forces users to create more complex and less predictable passwords, reducing the risk of simple passwords that are easy to exploit.

Decreasing the password expiration times (B) can encourage users to change their passwords more frequently but does not directly address the issue of password complexity. Enabling an automatic lock timer (C) can add a layer of security by locking accounts after a period of inactivity, but it does not improve the strength of the passwords themselves. Adding two characters to the minimum password length (D) can help to some extent by making passwords longer, but without requiring a mix of character types, passwords might still remain relatively easy to guess or crack.

---

### Question: 180

---

A user reports being unable to access a sports team's website on an office computer. The administrator tells the user this blocked access is intentional and based on company guidelines. Which of the following is the administrator referring to?

- A . NDA
- B . AUP
- C . VPN
- D . SOP

---

**Answer: B**

---

Explanation:

An AUP, or Acceptable Use Policy, is a set of rules applied by the owner, creator, or administrator of a network, website, or service that restricts the ways in which the network, website, or system may be used. In this scenario, the administrator is likely referring to the company's AUP, which outlines what employees can and cannot do on the company's network, including restrictions on accessing certain types of websites, such as sports teams' sites, for non-work-related purposes.

AUP (Acceptable Use Policy): This policy typically includes rules designed to maintain the security of the network, ensure the productivity of employees, and comply with legal regulations. Blocking access to specific websites is a common practice enforced through an AUP to align with these goals.

An NDA (Non-Disclosure Agreement) (A) is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes but wish to restrict access to or by third parties. A VPN (Virtual Private Network) (C) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. SOP (Standard Operating Procedures) (D) are a set of step-by-step instructions compiled by an organization to help workers carry out complex routine operations, which wouldn't typically include website access guidelines.

---

### Question: 181

---

A company installed WAPs and deployed new laptops and docking stations to all employees. The docking stations are connected via LAN cables. Users are now reporting degraded network service. The IT department has determined that the WAP mesh network is experiencing a higher than anticipated amount of traffic. Which of the following would be the most efficient way to ensure the wireless network can support the expected number of wireless users?

- A . Replacing non-mobile users' laptops with wired desktop systems
- B . Increasing the wireless network adapter metric
- C . Adding wireless repeaters throughout the building
- D . Upgrading the current mesh network to support the 802.11 n specification

---

**Answer: D**

---

Explanation:

When a WAP (Wireless Access Point) mesh network is experiencing a higher than anticipated amount of traffic, leading to degraded network service, upgrading the network to a more advanced wireless standard can help alleviate the problem. The 802.11n specification, also known as Wireless-N, offers significant improvements over earlier standards like 802.11b/g in terms of speed, range, and reliability. It allows for increased data throughput and better coverage, which can support a higher number of wireless users effectively.

Upgrading to 802.11n: This involves replacing existing WAPs with those that support the 802.11n standard or higher. The upgrade can result in improved network performance by accommodating more wireless connections with higher data rates, reducing congestion and improving overall network efficiency.

Replacing non-mobile users' laptops with wired desktop systems (A) could reduce wireless traffic but may not be feasible or desirable for all users. Increasing the wireless network adapter metric (B) would affect route priority but not overall network capacity. Adding wireless repeaters (C) can extend the range but might also introduce additional latency and does not necessarily increase the network's capacity to handle more users efficiently.

---

## **Question: 182**

---

A customer who uses a Linux OS called the help desk to request assistance in locating a missing file. The customer does not know the exact name of the file but can provide a partial file name. Which of the following tools should the technician use? (Select two).

- A . cat
- B . df
- C . grep
- D . ps
- E . dig
- F . find
- G . top

---

**Answer: C, F**

---

Explanation:

To locate a missing file with only a partial name known, the best tools to use in a Linux environment would be grep and find.

grep: This command is used to search the contents of files for a specific pattern. While grep itself might not be the first choice for finding file names, it can be combined with other commands (like ls or find) to search within file lists or contents.

find: This command is used to search for files in a directory hierarchy based on various criteria like name, size, modification date, etc. find can be used to search for files by partial name by using wildcards in the search pattern.

cat (A) is used to concatenate and display the content of files. df (B) displays the amount of disk space used and available on filesystems. ps (D) shows information about active processes. dig (E) is used for querying DNS name servers. top (G) displays Linux tasks and system performance information. None of these tools are directly suited for finding files by partial names.

---

## **Question: 183**

---

Users report having difficulty using the Windows Hello facial recognition feature. Which of the following is a secondary feature of Windows Hello that can be used to log in?

- A . Personal identification number
- B . Username/password
- C . One-time-use token
- D . Cryptographic device

---

**Answer: A**

---

### Explanation:

Windows Hello is a biometric-based technology that enables Windows 10 users to authenticate secure access to their devices, apps, online services, and networks with just a look or a touch. If users have difficulty using the facial recognition feature, Windows Hello also supports a Personal Identification Number (PIN) as a secondary feature for logging in. The PIN is tied to the specific device on which it is set up, adding a layer of security even if the PIN is obtained by someone else.

Personal identification number: The PIN serves as an alternative to the facial recognition feature, allowing users to quickly and securely access their devices without relying solely on biometric authentication.

Username/password (B) is the traditional method of authentication but is not specifically a secondary feature of Windows Hello. One-time-use token (C) and cryptographic device (D) could be part of an MFA setup but are not directly related to Windows Hello's alternate authentication options.

---

### Question: 184

---

A company using Active Directory wants to change the location of all users' 'Documents' to a file server on the network. Which of the following should the company set up to accomplish this task?

- A . Security groups
- B . Folder redirection
- C . Organizational unit structure
- D . Access control list

---

### Answer: B

---

### Explanation:

Folder redirection is a feature in Windows that allows administrators to change the default location of certain special folders within the user profile, such as the 'Documents' folder, to a different location, typically on a network server. This is commonly used in organizational environments to centralize file storage, simplify backups, and ensure data is stored on network drives with potentially more robust security measures and redundancy.

Folder redirection: By implementing folder redirection through Group Policy in Active Directory, a company can ensure that all users' 'Documents' folders are stored on a specified file server on the network, allowing for centralized management and backup of important user files.

Security groups (A) are used to manage user and computer access to shared resources, but they don't directly enable the relocation of user folders. Organizational unit structure (C) helps in managing and applying policies within Active Directory but is not directly related to the physical location of files. Access control lists (D) are used to define permissions for files and directories, but they do not govern where those files and directories should be located.

---

### Question: 185

---

A technician needs to strengthen security controls against brute-force attacks. Which of the following options best meets this requirement?

- A . Multifactor authentication
- B . Encryption
- C . Increased password complexity
- D . Secure password vault

---

**Answer: A**

---

Explanation:

Multifactor authentication (MFA) significantly enhances security by requiring two or more forms of verification before granting access to an account or system. This method is highly effective against brute-force attacks, where attackers attempt to guess a user's password through repeated trials. By implementing MFA, even if a password is compromised, unauthorized access is still prevented without the additional authentication factor(s), such as a code from a smartphone app, a fingerprint, or a physical security token.

Multifactor authentication: Provides an additional layer of security beyond just the password, making it much harder for attackers to gain unauthorized access through brute-force methods, as they would need to compromise more than one authentication factor.

Encryption (B) is crucial for protecting data at rest and in transit, but it does not directly prevent brute-force login attempts. Increased password complexity (C) can deter brute-force attacks by making passwords harder to guess, but it is not as effective as MFA in preventing access when passwords are compromised. A secure password vault (D) helps users manage and store their passwords securely, which can indirectly contribute to security by allowing users to keep more complex passwords, but it does not directly prevent brute-force attacks on accounts.

---

### **Question: 186**

---

A user takes a work-issued laptop home for the first time. When the user attempts to browse any website on the home internet, the user receives the following error:

'This site cannot be reached.'

A technician from work confirms that the static IP that was set up on the machine was changed back to DHCP. Which of the following needs to be corrected?

- A . HTTPS
- B . VLAN
- C . DNS
- D . SMTP

---

**Answer: C**

---

Explanation:

The error 'This site cannot be reached' often indicates a problem with DNS (Domain Name System) resolution, where the browser is unable to translate a website's domain name into its corresponding IP address. Since the laptop was set to use DHCP (Dynamic Host Configuration Protocol) at home, it's possible that it's not receiving the correct DNS

server information from the home network, or the DNS servers it was using at work are not accessible from the home network.

DNS: Checking and possibly correcting the DNS settings to ensure they are appropriate for the home network might resolve the browsing issue. The user can try using public DNS servers like those provided by Google (8.8.8.8 and 8.8.4.4) or Cloudflare (1.1.1.1) if the default DNS servers provided by the home ISP are not working properly.

HTTPS (A) is a protocol for secure communication over a computer network but is not something that needs to be configured on the user's end to solve this type of issue. VLAN (B) stands for Virtual Local Area Network and is more related to network segmentation and management within larger networks, not typically applicable to home internet issues. SMTP (D) stands for Simple Mail Transfer Protocol, which is used for sending emails, not for general web browsing issues.

---

### **Question: 187**

---

A user's Windows 10 workstation with an HDD is running really slowly. The user has opened, closed, and saved many large files over the past week. Which of the following tools should a technician use to remediate the issue?

- A . Disk Defragment
- B . Registry Editor
- C . System Information
- D . Disk Cleanup

---

### **Answer: A**

---

Explanation:

Over time, especially with frequent opening, modification, and saving of large files, a hard disk drive (HDD) can become fragmented. Fragmentation occurs when pieces of individual files are scattered across the disk, leading to longer read and write times, which can significantly slow down the computer. Disk defragmentation reorganizes these fragmented files, placing the pieces closer together on the drive, which improves access time and overall system performance.

Disk Defragment: Using the Disk Defragment tool on a Windows 10 system with an HDD will help in reorganizing the data more efficiently, thus potentially remedying the slow performance issue.

The Registry Editor (B) is a tool that allows for the viewing and editing of the Windows registry and is generally not used for performance improvement but rather for system settings and configuration adjustments. System Information (C) provides a detailed look at the computer's hardware and system details but does not offer tools for performance improvement. Disk Cleanup (D) can help free up space on the hard drive by removing temporary files and system files that are no longer needed, which can indirectly improve performance but is not the primary tool for addressing fragmentation.

---

### **Question: 188**

---

A user is experiencing the following issues with Bluetooth on a smartphone:

\* The user cannot hear any sound from a speaker paired with the smartphone.

\* The user is having issues synchronizing data from their smart watch, which is also connected via Bluetooth.

A technician checked the Bluetooth settings, confirmed it is successfully paired with a speaker, and adjusted the volume levels, but still could not hear anything. Which of the following steps should the technician take next to troubleshoot the Bluetooth issues?

- A . Restart the smartphone.
- B . Reset the network settings.
- C . Unpair the Bluetooth speaker.
- D . Check for system updates.

---

**Answer: A**

---

Explanation:

Restarting the smartphone can resolve a wide range of technical issues, including those related to Bluetooth connectivity. This simple step can refresh the system and eliminate temporary software glitches that might be interfering with Bluetooth functions like audio output and data synchronization.

Restart the smartphone: This action clears the system's RAM and can resolve conflicts between the Bluetooth service and other processes running on the smartphone, potentially fixing both the audio and synchronization issues.

Resetting network settings (B) could also potentially fix the issue but is a more drastic step that also clears Wi-Fi networks and passwords, cellular settings, and VPN configurations, which might not be necessary. Unpairing the Bluetooth speaker (C) could help if the issue is specific to the speaker, but since there are also synchronization issues with the smartwatch, the problem seems broader. Checking for system updates (D) is a good general maintenance step, but it's more likely to help with ongoing or known issues rather than immediate connectivity problems.

---

### **Question: 189**

---

A technician is setting up a network printer for a customer who has a SOHO router. The technician wants to make sure the printer stays connected in the future and is available on all the computers in the house. Which of the following should the technician configure on the printer?

- A . DNS settings
- B . Static IP
- C . WWAN
- D . Metered connection

---

**Answer: B**

---

Explanation:

Configuring a static IP address for a network printer in a SOHO (Small Office/Home Office) environment ensures that the printer maintains the same IP address over time. This consistency is crucial for networked devices like printers, as

computers and other devices rely on this specific address to connect to the printer. If the printer's IP address were to change (as it might with DHCP), devices would no longer be able to communicate with it without reconfiguration.

**Static IP:** Assigning a static IP address to the printer ensures it always uses the same IP, making it reliably accessible to all computers in the house regardless of network changes or router reboots.

---

### Question: 190

---

A user is trying to limit the amount of time their children spend on the internet. Which of the following Windows 10 settings should be enabled to accomplish this objective?

- A . Family Options
- B . Update & Security
- C . Ease of Access
- D . Network & Internet
- E . Privacy

---

### Answer: A

---

Explanation:

Windows 10 includes a set of parental controls within the 'Family Options' section of the Windows settings. This feature allows parents to manage their children's computing activities, including setting time limits on device use, filtering web content, managing privacy and online safety settings, and viewing activity reports.

**Family Options:** By enabling and configuring Family Options, the user can set specific times when their children can use the device and access the internet, effectively limiting their overall screen time and internet usage.

**Update & Security (B)** mainly deals with Windows updates and security features but does not directly provide settings for time management. **Ease of Access (C)** is focused on accessibility settings and does not include time management options. **Network & Internet (D)** settings control network connectivity and do not offer parental controls or time limits. **Privacy (E)** settings manage which applications can access device features and user data but do not include time management options.

---

### Question: 191

---

A customer, whose smartphone's screen was recently repaired, reports that the device has no internet access through Wi-Fi. The device shows that it is connected to Wi-Fi, has an address of 192.168.1.42. and has no subnet mask. Which of the following should the technician check next?

- A . Internal antenna connections
- B . Static IP settings
- C . Airplane mode
- D . Digitizer calibration

---

**Answer: A**

---

Explanation:

Given that the smartphone's screen was recently repaired and now experiences issues with Wi-Fi connectivity, despite showing that it is connected to a network, the problem could be related to the internal antenna connections that might have been disturbed or disconnected during the repair process.

**Internal Antenna Connections:** Smartphones use internal antennas for Wi-Fi and cellular connections. If these antennas are not properly connected, the device may show as connected to a Wi-Fi network but fail to transmit data effectively, resulting in no internet access.

Checking static IP settings (B) would be relevant if the device were not obtaining an IP address at all, but the device does have an IP address. Airplane mode (C) would prevent the device from connecting to Wi-Fi networks entirely. Digitizer calibration (D) is related to the touchscreen functionality and would not affect Wi-Fi connectivity.

---

**Question: 192**

---

A malicious user was able to export an entire website's user database by entering specific commands into a field on the company's website. Which of the following did the malicious user most likely exploit to extract the data?

- A . Cross-site scripting
- B . SQL injection
- C . Brute-force attack
- D . DDoS attack

---

**Answer: B**

---

Explanation:

SQL injection is a type of attack that takes advantage of vulnerabilities in a web application's database query software, allowing an attacker to send malicious SQL commands through the application to the database. These commands can manipulate the database and can lead to unauthorized data access or manipulation.

**SQL injection:** In the scenario described, the malicious user was able to export an entire website's user database by entering specific commands into a field on the company's website, which is a classic example of an SQL injection attack. This type of attack exploits vulnerabilities in the database layer of an application to execute unauthorized SQL commands.

Cross-site scripting (A) involves injecting malicious scripts into content from otherwise trusted websites. A brute-force attack (C) is an attempt to gain access to a system by systematically checking all possible keys or passwords until the correct one is found. A DDoS attack (D) is an attempt to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of internet traffic.

---

### **Question: 193**

---

An organization wants to deploy a customizable operating system. Which of the following should the organization choose?

- A . Windows 10
- B . macOS
- C . Linux
- D . Chrome OS
- E . iOS

---

**Answer: C**

---

Explanation:

Linux is known for its high degree of customizability and flexibility, making it an ideal choice for organizations looking to deploy a customizable operating system. Unlike proprietary operating systems, Linux allows users to modify or replace almost any part of the system, from the kernel to the desktop environment and applications, to suit their specific needs.

Linux: This open-source operating system provides access to the source code, enabling extensive customization. Organizations can tailor Linux distributions to fit specific requirements, making it a popular choice for servers, specialized workstation environments, and embedded systems.

Windows 10 (A) and macOS (B) offer some level of customization but are more restricted due to their proprietary nature. Chrome OS (D) is designed for simplicity and security, focusing on web applications, which limits deep system-level customizations. iOS (E) is designed for Apple's mobile devices and is not applicable for organizational deployment beyond mobile and tablet devices; it also offers limited customization compared to Linux.

---

### **Question: 194**

---

A technician has been unable to remediate a persistent malware infection on a user's workstation. After the technician reinstalled the OS, the malware infection returned later that day. Which of the following is the most likely source?

- A . Trojan
- B . Boot sector virus
- C . Spyware
- D . Rootkit

---

**Answer: B**

---

Explanation:

A boot sector virus infects the master boot record (MBR) of a hard drive, the sector that contains information required to start the operating system after the computer is turned on. This type of virus is particularly insidious because it loads into memory immediately upon booting and before most antivirus programs start. This makes it

possible for the virus to evade detection and removal, and can easily reinfect a system even after the operating system is reinstalled if the boot sector is not cleaned.

**Boot sector virus:** Given that the malware infection returned after the OS reinstallation, it's likely that the virus was not removed from the boot sector during the reinstallation process. Reinstalling the OS without cleaning the boot sector won't remove the infection, allowing the virus to continue to affect the system.

Other options:

**Trojan:** A Trojan is a type of malware that disguises itself as legitimate software. While Trojans can be persistent, the reinstallation of the OS should remove any Trojans unless they are reintroduced after installation.

**Spyware:** Spyware is designed to gather information about a person or organization without their knowledge. Like Trojans, spyware should be removed with an OS reinstallation unless it is reintroduced in some way.

**Rootkit:** Rootkits are designed to enable continued privileged access to a computer while actively hiding their presence. While a rootkit could potentially survive an OS reinstall if it infects the firmware or certain areas outside the OS, the scenario described points more specifically to a boot sector virus, especially considering the immediate return of the infection after OS reinstallation.

---

### **Question: 195**

---

Which of the following combinations meets the requirements for mobile device multifactor authentication?

- A . Password and PIN
- B . Password and swipe
- C . Fingerprint and password
- D . Swipe and PIN

---

**Answer: C**

---

Explanation:

Multifactor authentication (MFA) requires the use of two or more verification factors to gain access to a resource such as an application, online account, or a VPN. The factors are categorized into something you know (like a password or PIN), something you have (like a security token or a smartphone), and something you are (like a biometric verification such as a fingerprint).

**Fingerprint and password:** This combination meets the criteria for MFA as it uses two different categories of authentication factors: 'something you are' (fingerprint) and 'something you know' (password). This enhances security by combining two distinct methods of authentication.

Other combinations mentioned:

**Password and PIN:** Both of these factors fall under the same category of 'something you know,' and hence, do not constitute multifactor authentication.

**Password and swipe:** Swiping a pattern is similar to a password in that it is something you know, so this does not qualify as multifactor authentication.

Swipe and PIN: Again, both of these are 'something you know' and do not qualify as multifactor authentication since they fall under the same category.

---

### Question: 196

---

Which of the following Linux commands would help to identify which directory the user is currently operating in?

- A . pwd
- B . dig
- C . find
- D . cat

---

**Answer: A**

---

Explanation:

The `pwd` command, which stands for 'print working directory,' is used in Linux and Unix-like operating systems to display the current directory in which the user is operating. This command outputs the full pathname of the current working directory, helping users to understand their current location in the filesystem hierarchy.

`pwd`: When executed, it provides the absolute path of the directory you're currently in, which is useful for navigation and scripting purposes.

Other options listed:

`dig`: This command is used for querying DNS name servers for information about host addresses, mail exchanges, name servers, and related information.

`find`: This command is used to search for files in a directory hierarchy based on specified criteria (such as name, modification date, size, etc.).

`cat`: Short for 'concatenate,' this command is used to read the contents of files and output them to the terminal.

---

### Question: 197

---

A technician is setting up a printer on a Linux workstation. Which of the following commands should the technician use to set the default printer?

- A . `ipr`
- B . `lspool`
- C . `lpstat`
- D . `lpoptions`

---

**Answer: A**

---

Explanation:

In Linux, the `lp` command is used to manage print jobs, including setting the default printer. The `lp` command allows users to send print jobs to a printer queue, check the status of print jobs, and cancel print jobs, among other functionalities. By using options and parameters with the `lp` command, a technician can specify a particular printer as the default for future print jobs, ensuring that documents are routed to the correct printer without needing to specify it each time.

---

### Question: 198

---

When a user attempts to open an email using a company-issued smartphone, the user receives a message stating the email is encrypted and cannot be opened. The user forwards the email to a personal account and receives the same message. The user then contacts the IT department for assistance. The technician instructs the user to contact the sender to exchange information in order to decode the message. Which of the following will the user receive from the sender?

- A . Keys
- B . Token
- C . Password
- D . RootCA

---

**Answer: A**

---

Explanation:

When an email is encrypted and the recipient cannot open it, the issue typically revolves around the need for encryption keys. Encryption keys are used to encode and decode the email content, ensuring that only authorized recipients with the correct key can access the information. In this scenario, the user would need to receive the appropriate decryption key from the sender to unlock and read the encrypted email. This exchange ensures that sensitive information remains secure during transmission and is only accessible to intended recipients.

---

### Question: 199

---

A company wants to take advantage of modern technology and transition away from face-to-face meetings. Which of the following types of software would benefit the company the most? (Select two).

- A . Videoconferencing
- B . File transfer
- C . Screen-sharing
- D . Financial
- E . Remote access
- F . Record-keeping

---

**Answer: A, C**

---

Explanation:

For a company looking to transition away from face-to-face meetings, videoconferencing and screen-sharing software would be most beneficial.

Videoconferencing software allows participants to conduct virtual meetings with audio and video capabilities, effectively simulating a face-to-face interaction without the need for physical presence. This can greatly reduce travel costs and time while maintaining the personal touch of meetings.

Screen-sharing enables participants in a virtual meeting to view one another's computer screens in real time. This is particularly useful for presentations, collaborative work, and troubleshooting, as it allows for a more interactive and engaging meeting experience.

Both technologies support the company's goal of leveraging modern technology to enhance communication and collaboration while reducing reliance on physical meetings.

---

### **Question: 200**

---

A user wants to back up a device's OS and data

a. Which of the following is the best way to accomplish this task?

- A . Incremental backup
- B . System image
- C . System restore point
- D . Differential backup

---

**Answer: B**

---

Explanation:

A system image is a complete snapshot of everything on a device's storage at a given point in time, including the operating system, installed programs, system settings, and all user files. This method is the best way to back up the OS and data comprehensively because it allows for the restoration of a system to its exact state at the time the image was taken. This is particularly useful in disaster recovery scenarios where it's crucial to restore a system quickly and efficiently to minimize downtime.

---

### **Question: 201**

---

A technician needs to upgrade a legacy system running on a 32-bit OS with new applications that can work both on a 32-bit and a 64-bit system. The legacy system is critically important to the organization. The IT manager cautions that the new applications must not have a detrimental effect on company finances. Which of the following impacts is the IT manager most concerned with?

- A . Device
- B . Business
- C . Network
- D . Operation

---

**Answer: B**

---

Explanation:

The IT manager's caution regarding the new applications not having a detrimental effect on company finances points directly to concerns about the business impact. This encompasses potential costs associated with upgrading legacy systems, compatibility issues that might arise from running new applications on old infrastructure, and the risks of system downtime or reduced performance affecting business operations. The focus here is on ensuring that the integration of new applications into the legacy system does not incur unexpected expenses or disrupt critical business processes.

---

### **Question: 202**

---

A technician is configuring a SOHO router and wants to only allow specific computers on the network. Which of the following should the technician do?

- A . Configure MAC filtering.
- B . Disable DHCP.
- C . Configure port forwarding.
- D . Disable guest access.

---

**Answer: A**

---

Explanation:

For a SOHO (Small Office/Home Office) router setup where the goal is to only allow specific computers on the network, MAC filtering is the appropriate solution:

Configure MAC filtering: This security measure involves creating a list of allowed device MAC (Media Access Control) addresses in the router's settings. Only devices with MAC addresses on this list will be able to connect to the network, effectively restricting access to authorized computers only.

---

### **Question: 203**

---

A user's computer is running slower than usual and takes a long time to start up. Which of the following tools should the technician use first to investigate the issue?

- A . Action Center
- B . Task Manager
- C . Resource Monitor
- D . Security Configuration Wizard
- E . Event Viewer

---

**Answer: B**

---

Explanation:

When a computer is running slower than usual and experiences long startup times, the first tool to use is:

Task Manager: This utility provides real-time data on the processes and applications consuming system resources like CPU, memory, and disk usage. By identifying resource-heavy processes, a technician can take steps to optimize performance or identify malicious software.

---

### **Question: 204**

---

A technician wants to securely dispose of storage drives. Which of the following is the best way to eliminate data on SSDs?

- A . Degaussing
- B . Shredding
- C . Erasing
- D . Drilling

---

**Answer: B**

---

Explanation:

For securely disposing of SSDs, physical destruction methods like shredding are considered most effective:

Shredding: This method involves physically breaking the SSD into small pieces, making data recovery practically impossible. It's a recommended practice for ensuring that sensitive data on SSDs is irretrievably destroyed.

---

### **Question: 205**

---

A user reports receiving constant, unwanted pop-ups and being unable to close the browser window. These issues have impacted the user's productivity and may have caused the user's files to be altered. Which of the following should a technician do to address these issues with minimal impact to the user?

- A . Use System Restore to recover the OS files.
- B . Wipe the computer and install a new copy of the OS.
- C . Identify whether the disk partition table has been reduced in size.
- D . Perform a full-system, antivirus scan and check browser notifications.

---

**Answer: D**

---

Explanation:

For issues related to constant, unwanted pop-ups and browser window problems, a careful approach that minimizes impact to the user's data and productivity is advisable:

Perform a full-system, antivirus scan: This step involves using antivirus software to scan the entire system for malware or adware that might be causing the pop-ups and browser issues.

Check browser notifications: Some unwanted pop-ups may result from browser notification permissions inadvertently granted to malicious or spammy websites. Reviewing and adjusting these settings can help stop the pop-ups.

---

### **Question: 206**

---

A user recently downloaded a free game application on an Android device. The device then began crashing frequently and quickly losing its battery charge. Which of the following should the technician recommend be done first to remediate these issues? (Select two).

- A . Uninstall the game application.
- B . Perform a factory reset of the device.
- C . Connect the device to an external charger.
- D . Install the latest security patches.
- E . Clear the application's cache.
- F . Enable the device's built-in anti-malware protection.

---

**Answer: A, D**

---

Explanation:

When an Android device starts exhibiting issues like frequent crashes and rapid battery drain after downloading an application, the first step should be to address the immediate cause:

Uninstall the game application: Since the issues started after the game application was installed, removing it is a logical first step. Unwanted or malicious applications can cause such symptoms by running harmful processes in the background or exploiting system resources.

Install the latest security patches: Keeping the device updated with the latest security patches is crucial for protecting against vulnerabilities that could be exploited by malicious software. Updating can resolve existing security flaws and improve device stability.

---

### **Question: 207**

---

A technician is troubleshooting a Windows system that is having issues with the OS loading at startup. Which of the following should the technician do to diagnose the issue?

- A . Enable boot logging on the system.
- B . Launch the last known-good configuration.
- C . Check the system resource usage in Task Manager.
- D . Run the sfc /scannow command.

E . Use the Event Viewer to open the application log

---

**Answer: A**

---

Explanation:

When troubleshooting a Windows system that is experiencing issues during the OS loading phase at startup, enabling boot logging is a practical step. Boot logging creates a record of all drivers and services that are loaded (or attempted to be loaded) during the startup process. This record, typically named ntbtlog.txt, can be reviewed to identify any drivers or services that failed to load, which could be contributing to the startup issues. This diagnostic step helps pinpoint the problematic component(s) and facilitates targeted troubleshooting to resolve the OS loading issues.

---

### **Question: 208**

---

A user receives an error message on a Windows 10 device when trying to access a mapped drive from a Windows XP machine in the office. Other Windows XP devices in the office can access the drive. Which of the following Control Panel utilities should the user select to enable connectivity to the device?

- A . Devices and Printers
- B . Administrative Tools
- C . Network and Sharing Center
- D . Programs and Features

---

**Answer: C**

---

Explanation:

The Network and Sharing Center in the Control Panel is the central place to manage network connections and settings in Windows. When facing issues with accessing a mapped drive, this utility allows users to review and adjust network settings, making it possible to resolve connectivity problems. It provides options to view network status, set up new connections, change adapter settings, and troubleshoot network problems, which can help in enabling connectivity to the mapped drive on the Windows XP machine.

---

### **Question: 209**

---

A technician is doing a bare-metal installation of the Windows 10 operating system. Which of the following prerequisites must be in place before the technician can start the installation process?

- A . Internet connection
- B . Product key
- C . Sufficient storage space
- D . UEFI firmware
- E . Legacy BIOS

**Explanation:**

Before starting a bare-metal installation of Windows 10, ensuring that there is sufficient storage space on the system's hard drive or SSD is crucial. This is because the installation files need enough room to be copied and for the operating system to be installed and function properly. Without adequate storage, the installation process can fail or the operating system might not perform optimally. Other prerequisites like internet connection, product key, and specific firmware types might be necessary at different stages of installation or activation, but the fundamental requirement is enough storage space to accommodate the new OS.

---

**Question: 210**

---

A technician needs to recommend a way to keep company devices for field and home-based staff up to date. The users live in various places across the country and the company has several national offices that staff can go to for technical support. Which of the following methods is most appropriate for the users?

- A . Make office attendance mandatory for one day per week so that updates can be installed.
- B . Ask users to ensure that they run updates on devices and reboot computers on a regular basis.
- C . Push updates out via VPN on a weekly basis in a staggered manner so that the network is not affected.
- D . Configure cloud-based endpoint management software to automatically manage computer updates.

**Explanation:**

For a company with geographically dispersed staff and the need to keep devices updated, using cloud-based endpoint management software is the most efficient method. This type of software allows IT administrators to remotely manage and push updates to company devices, regardless of their location. It ensures that all devices remain up to date with the latest security patches and software updates without requiring physical access or user intervention. This approach is scalable, reduces the risk of unpatched vulnerabilities, and is convenient for both the IT department and the end-users.

---

**Question: 211**

---

A user is setting up a new Windows 10 laptop. Which of the following Windows settings should be used to input the SSID and password?

- A . Network & Internet
- B . System
- C . Personalization
- D . Accounts

---

**Answer: A**

---

Explanation:

In Windows 10, the 'Network & Internet' settings category is where users can manage all network-related configurations, including Wi-Fi connections. To connect to a Wi-Fi network, users need to input the network's SSID (Service Set Identifier) and the corresponding password. This section allows users to view available networks, enter credentials for secure networks, and manage other network features such as airplane mode, VPN, and mobile hotspot settings.

---

**Question: 212**

---

A technician receives a high-priority ticket about sensitive information collected from an end user's workstation. Which of the following steps should a technician take to preserve the chain of custody for a forensic investigation?

- A . Reimage the workstation.
- B . Inform the user of the investigation.
- C . Recover and secure the workstation.
- D . Back up the workstation

---

**Answer: C**

---

Explanation:

In the context of a forensic investigation, especially involving sensitive information, preserving the integrity and the chain of custody of the potential evidence is crucial. The step to 'Recover and secure the workstation' involves physically securing the workstation to prevent any unauthorized access and logically securing the data by ensuring that no changes are made to the system or files. This step helps maintain the original state of the workstation, which is essential for a legitimate forensic analysis and ensuring that the evidence is admissible in legal proceedings.

---

**Question: 213**

---

Which of the following is used to generate passcodes necessary to access applications or systems that require an extra layer of security?

- A . Authenticator application
- B . Access control lists
- C . Biometrics
- D . Smart card readers

---

**Answer: A**

---

Explanation:

Authenticator applications are designed to enhance security by generating temporary, time-sensitive passcodes used in two-factor authentication (2FA) processes. These passcodes are used in conjunction with traditional credentials (like usernames and passwords) to grant access to systems or applications. This extra layer of security ensures that even if primary login credentials are compromised, unauthorized access is still prevented without the dynamically generated code from the authenticator app.

---

### Question: 214

---

A technician is troubleshooting a smartphone that is unable to download and install the latest OS update. The technician notices the device operates more slowly than expected, even after rebooting and closing all applications. Which of the following should the technician check next?

- A . Application permissions
- B . Available storage space
- C . Battery charge level
- D . Wi-Fi connection speed

---

### Answer: B

---

Explanation:

When a smartphone is unable to download and install the latest OS update and is operating slower than expected, one of the first things to check is the available storage space. Operating system updates often require a significant amount of free space for downloading and installing, and insufficient space can prevent the update process from initiating or completing.

**Available Storage Space:** Smartphones use their internal storage to hold the OS, apps, user data, and temporary files needed for updates. If the storage is nearly full, the device can slow down due to the lack of space for writing temporary files and may not have enough space to download and install updates. Clearing up space can resolve these issues.

Checking application permissions (A) might be relevant for specific app-related issues but is less likely to affect OS updates. The battery charge level (C) can affect the initiation of an update, as some devices require a minimum charge level to start the update process, but it doesn't typically cause slow operation. While a stable Wi-Fi connection (D) is necessary for downloading updates, it's less likely to be the cause of slowed operation and update issues compared to insufficient storage space.:.

---

### Question: 215

---

A technician is troubleshooting a PC that is unable to perform DNS lookups. Utilizing the following firewall output:

Protocol/Port Action Direction

1 Allow Out

445 Block Out

53 Block Out

123 Block Out

80 Block Out

Which of the following ports should be opened to allow for DNS recursion?

- A . 1
- B . 53
- C . 80
- D . 123
- E . 445

---

**Answer: B**

---

Explanation:

DNS (Domain Name System) lookups are essential for translating human-friendly domain names into IP addresses that computers use to communicate. DNS typically uses port 53 for its communication.

In the provided firewall output, various ports are either allowed or blocked for outgoing traffic. For DNS recursion, which is the process of resolving domain names to IP addresses, port 53 must be open.

Port 53: This is the standard port used by DNS for queries and responses. The fact that it is currently blocked (as per the firewall output) is the reason why DNS lookups are failing. Opening port 53 will allow the DNS requests to pass through the firewall, enabling the resolution of domain names to IP addresses.

Other ports mentioned in the output are used for different services and protocols:

Port 1 is generally not used for standard services.

Port 445 is associated with SMB (Server Message Block) for file sharing in Windows environments.

Port 123 is used by NTP (Network Time Protocol) for time synchronization.

Port 80 is used for HTTP traffic, which is web traffic but not related to DNS lookups.

---

### **Question: 216**

---

An administrator needs to select a method to dispose of SSDs containing sensitive data.

a. Which of the following are the most appropriate methods? (Select two).

- A . Degauss
- B . Delete
- C . Incinerate
- D . Recycle
- E . Format
- F . Shred

---

**Answer: C, F**

---

Explanation:

Disposing of SSDs (Solid State Drives) containing sensitive data requires methods that ensure the data cannot be recovered. SSDs store data on flash memory, which makes traditional data destruction methods like degaussing ineffective, as degaussing relies on demagnetizing the magnetic media found in traditional hard drives.

**Incineration:** This method ensures the complete destruction of the SSD by burning it at high temperatures. This process is effective as it physically destroys the flash memory chips, making data recovery impossible.

**Shredding:** Shredding involves physically breaking the SSD into small pieces. Specialized shredding machines designed for electronic media can cut the SSD into pieces small enough to render the data unrecoverable.

Other listed options such as Degaussing (A) is ineffective on SSDs because they don't use magnetic storage. Simple Deletion (B) and Formatting (E) are not secure methods for data destruction as the data can potentially be recovered using specialized software. Recycling (D) is environmentally friendly but does not guarantee data destruction if the drive is not physically destroyed first.

---

### **Question: 217**

---

An IT technician is attempting to access a user's workstation on the corporate network but needs more information from the user before an invitation can be sent. Which of the following command-line tools should the technician instruct the user to run?

- A . nslookup
- B . tracert
- C . hostname
- D . gpresult

---

**Answer: C**

---

Explanation:

The hostname command-line tool is used to display the name of the local machine. This information can be crucial for identifying the device within a network, especially when setting up remote access or sharing resources like folders and printers. Unlike other command-line tools that provide more detailed network diagnostics or configuration details, hostname straightforwardly offers the device's network identification, making it suitable for the scenario described.

Topic 6, Exam Pool F (NEW)

---

### **Question: 218**

---

A user reports that an air-gapped computer may have been infected with a virus after the user transferred files from a USB drive. The technician runs a computer scan with Windows Defender but does not find an infection. Which of the following actions should the technician take next? (Select two).

- A . Examine the event logs.
- B . Connect to the network.
- C . Document the findings.
- D . Update the definitions.
- E . Reimage the computer.
- F . Enable the firewall.

---

**Answer: A, D**

---

Explanation:

When dealing with a suspected virus infection on an air-gapped computer, after an initial scan with Windows Defender shows no infection, the next steps should include examining the event logs to look for suspicious activity and updating the virus definitions for a more thorough scan. Event logs can provide insights into system changes and potential malicious activities, while updated definitions ensure the antivirus software can detect the latest threats. Connecting to the network or enabling the firewall might not be appropriate due to the risk of spreading the infection, and re-imaging the computer or documenting the findings would be subsequent steps if the initial actions don't resolve the issue. Reference: Official CompTIA A+ Core 1 and Core 2 Student Guide.

---

### **Question: 219**

---

A student is setting up a new Windows 10 laptop for the upcoming semester. The student is interested in customizing the wallpaper. Which of the following should the student use to change the wallpaper?

- A . Apps and Features
- B . Personalization
- C . File Explorer
- D . Task Manager

---

**Answer: B**

---

Explanation:

To change the wallpaper on a Windows 10 laptop, the 'Personalization' settings should be used. These settings allow users to customize themes, which include various aspects of the desktop environment such as the desktop wallpaper, screen saver, color scheme, and more. This makes 'Personalization' the correct option for customizing the wallpaper. Reference: Official CompTIA A+ Core 1 and Core 2 Student Guide.

---

### **Question: 220**

---

Which of the following operating systems would most likely be used to run the inventory management system at a factory?

- A . Windows
- B . Chrome OS
- C . Android
- D . iOS

---

**Answer: A**

---

Explanation:

Windows is widely used in industrial and business environments due to its major market presence, extensive support from the industry, and a broad selection of operating system options. It supports a wide variety of software, making it suitable for running complex systems like an inventory management system in a factory. Other options such as Chrome OS, Android, and iOS are either more consumer-oriented or designed for specific types of devices, making them less likely choices for an industrial application like inventory management. Reference: Professor Messer's CompTIA 220-1102 A+ Course Notes.

---

### **Question: 221**

---

Which of the following languages is used for scripting the creation of Active Directory accounts?

- A . Bash
- B . SQL
- C . PHP
- D . PowerShell

---

**Answer: D**

---

Explanation:

PowerShell is a scripting language that can interact with Active Directory and other Windows components. It has a built-in cmdlet called New-ADUser that can create user accounts in Active Directory. PowerShell can also use the Active Directory module to access other AD-related functions and attributes. Other languages, such as Bash, SQL, and PHP, are not designed for creating Active Directory accounts and would require additional tools or libraries to do so.

---

### **Question: 222**

---

Which of the following are mobile operating systems used on smartphones? (Select two).

- A . macOS
- B . Windows
- C . Chrome OS
- D . Linux

- E . iOS
- F . Android

---

**Answer: E, F**

---

Explanation:

iOS and Android are the two most popular and widely used mobile operating systems for smartphones. They are both based on Unix-like kernels and provide a variety of features and applications for users and developers. iOS is developed by Apple and runs exclusively on Apple devices, such as iPhones and iPads. Android is developed by Google and runs on a range of devices from different manufacturers, such as Samsung, Huawei, and Motorola. The other options are not mobile operating systems for smartphones, but rather for other types of devices or platforms. macOS is a desktop operating system for Apple computers, such as MacBooks and iMacs. Windows is a desktop operating system for Microsoft computers, such as Surface and Dell. Chrome OS is a web-based operating system for Google devices, such as Chromebooks and Chromecast. Linux is a family of open-source operating systems for various devices and platforms, such as Ubuntu, Fedora, and Raspberry Pi.

---

### **Question: 223**

---

A client wants a technician to set up a proxy server in a branch office to manage internet access. This involves configuring the workstations to use the new proxy server. Which of the following Internet Options tabs in Control Panel would be most appropriate for the technician to use to configure the settings?

- A . Privacy
- B . Advanced
- C . Content
- D . Connections
- E . Security

---

**Answer: D**

---

Explanation:

[The Connections tab in Internet Options allows the technician to configure the proxy server settings for the workstations. The technician can enter the proxy server address and port number, and specify which websites to bypass the proxy server for. The other tabs are not relevant for configuring the proxy server settings. Reference: CompTIA A+ Certification Exam Core 2 Objectives, page 9, section 1.7; CompTIA A+ Core 2 \(220-1102\) Certification Study Guide, page 140, section 1.7.](#)

---

### **Question: 224**

---

A user's laptop has been performing slowly and redirecting to unfamiliar websites. The user has also noticed random pop-up windows. Which of the following is the first step a technician should take to resolve the issue?

- A . Scan for malware and ransomware.

- B . Perform a system restore.
- C . Check the network utilization.
- D . Update the antivirus software.

---

**Answer: A**

---

Explanation:

The most likely cause of the user's laptop issues is that it has been infected by some type of malware or ransomware. Malware and ransomware are malicious software that can harm, exploit, or disrupt devices or networks<sup>12</sup>. They can cause symptoms such as slow performance, browser redirects, pop-up windows, data encryption, or ransom demands<sup>12</sup>. Therefore, the first step a technician should take to resolve the issue is to scan the laptop for malware and ransomware using a reliable and updated anti-malware tool<sup>34</sup>. This can help identify and remove any malicious software that may be present on the laptop. Scanning for malware and ransomware is more effective and urgent than the other options because:

Performing a system restore may not remove the malware or ransomware, as some of them can persist or hide in the system files or backup copies<sup>34</sup>. Moreover, a system restore may result in data loss or corruption, as it restores the system to a previous state and deletes any changes made after that point<sup>5</sup>.

Checking the network utilization may not help diagnose or fix the problem, as the malware or ransomware may not be using the network at all, or may be using it in a stealthy or encrypted manner<sup>34</sup>. Furthermore, checking the network utilization does not address the root cause of the issue, which is the presence of malicious software on the laptop.

Updating the antivirus software may not be sufficient to detect or remove the malware or ransomware, as some of them may evade or disable the antivirus software, or may be too new or unknown for the antivirus software to recognize<sup>34</sup>. Additionally, updating the antivirus software does not guarantee that the laptop will be scanned for malware or ransomware, as the user may need to initiate or schedule the scan manually.

---

### **Question: 225**

---

Which of the following is the best way to limit the loss of confidential data if an employee's company smartphone is lost or stolen?

- A . Installing a VPN
- B . Implementing location tracking
- C . Configuring remote wipe
- D . Enabling backups

---

**Answer: C**

---

Explanation:

Configuring remote wipe allows the device owner or administrator to erase all the data on the device remotely, in case it is lost or stolen. This prevents unauthorized access to confidential data and reduces the risk of data breaches. Installing a VPN, implementing location tracking, and enabling backups are useful features, but they do not directly

[limit the loss of data if the device is compromised. Reference: CompTIA A+ Certification Exam Core 2 Objectives, Domain 2.0: Security, Objective 2.5: Given a scenario, use methods to secure mobile devices.](#)

---

### Question: 226

---

A management team at a small office wants to block access to inappropriate websites and create a log of these access attempts. Which of the following is a way to meet these requirements?

- A . Content filter
- B . Screened subnet
- C . Port forwarding
- D . Access control list

---

**Answer: A**

---

Explanation:

A content filter is a device or software that blocks or allows access to web pages based on predefined criteria, such as keywords, categories, or ratings. A content filter can also create a log of the blocked or allowed web requests, which can help the management team monitor and audit the web usage of their employees. A content filter is different from the other options because:

A screened subnet is a network segment that is protected by two firewalls, one facing the internet and one facing the internal network. A screened subnet can isolate servers or hosts that need to be accessed from both sides, such as a web server or a bastion host. A screened subnet does not filter web content based on predefined criteria, but rather on network addresses, ports, and protocols.

Port forwarding is a technique that allows a router to forward packets from one port to another port, usually on a different device. Port forwarding can enable remote access to services or applications that are hosted on a private network, such as a web server or a game server. Port forwarding does not filter web content based on predefined criteria, but rather on destination ports and addresses.

An access control list (ACL) is a set of rules that defines which packets are allowed or denied on a network device, such as a router or a firewall. An ACL can filter packets based on source and destination addresses, ports, protocols, and other criteria. An ACL can also create a log of the matched or unmatched packets, which can help the management team troubleshoot and secure their network. An ACL does not filter web content based on predefined criteria, but rather on packet headers and fields.

---

### Question: 227

---

A remote user's smartphone is performing very slowly. The user notices that the performance improves slightly after rebooting but then reverts back to performing slowly. The user also notices that the phone does not get any faster after connecting to the company's corporate guest network. A technician sees that the phone has a large number of applications installed on it. Which of the following is the most likely cause of the issue?

- A . The user is in a poor signal area.

- B . The user has too many processes running.
- C . The smartphone has malware on it.
- D . The smartphone has been jailbroken.

---

**Answer: B**

---

Explanation:

One of the common reasons for a slow smartphone performance is having too many apps installed and running in the background. These apps consume the device's memory (RAM) and CPU resources, which can affect the speed and responsiveness of the phone. Rebooting the phone can temporarily clear the RAM and stop some background processes, but they may resume after a while. Connecting to a different network does not affect the performance of the phone, unless the network is congested or has a poor signal. The user can improve the phone's performance by uninstalling unused apps, clearing app caches, and restricting background activities<sup>1</sup>. Malware can also slow down a phone, but it is not the most likely cause in this scenario, as the user does not report any other symptoms of infection, such as pop-ups, battery drain, or data usage spikes<sup>2</sup>. Jailbreaking a phone can also affect its performance, but it is not a cause, rather a consequence, of the user's actions. Jailbreaking is the process of removing the manufacturer's restrictions on a phone, which allows the user to install unauthorized apps, customize the system, and access root privileges<sup>3</sup>. However, jailbreaking also exposes the phone to security risks, voids the warranty, and may cause instability or compatibility issues<sup>4</sup>.

Reference 1: Speed up a slow Android device - Android Help - Google Help 2: Why your phone slows down over time and what you can do to stop it | TechRadar 3: How to tell if your phone has a virus | Norton 4: What is Jailbreaking? - Definition from Techopedia 5: What is Jailbreaking an iPhone? - Lifewire

---

### **Question: 228**

---

An employee has repeatedly contacted a technician about malware infecting a work computer. The technician has removed the malware several times, but the user's PC keeps getting infected. Which of the following should the technician do to reduce the risk of future infections?

- A . Configure the firewall.
- B . Restore the system from backups.
- C . Educate the end user
- D . Update the antivirus program.

---

**Answer: C**

---

Explanation:

Malware is software that infects computer systems to damage, disable or exploit the computer or network for various malicious purposes<sup>5</sup>. Malware is typically distributed via email attachments, fake internet ads, infected applications or websites, and often relies on user interaction to execute<sup>6</sup>. Therefore, one of the most effective ways to prevent malware infections is to educate the end user about the common signs and sources of malware, and how to avoid them<sup>7</sup>. Configuring the firewall, restoring the system from backups, and updating the antivirus program are also important security measures, but they do not address the root cause of the user's repeated infections, which is likely due to a lack of awareness or caution.

### Question: 229

---

Which of the following Windows 10 editions is the most appropriate for a single user who wants to encrypt a hard drive with BitLocker?

- A . Professional
- B . Home
- C . Enterprise
- D . Embedded

---

**Answer: A**

---

Explanation:

[BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices](#)<sup>1</sup>. [BitLocker is available on supported devices running Windows 10 or 11 Pro, Enterprise, or Education](#)<sup>2</sup>. [Windows 10 Home does not support BitLocker](#)<sup>3</sup>, and [Windows 10 Embedded is designed for specialized devices and does not offer BitLocker as a feature](#)<sup>4</sup>. Therefore, the most appropriate Windows 10 edition for a single user who wants to encrypt a hard drive with BitLocker is Professional.

[Reference 1: BitLocker overview - Windows Security | Microsoft Learn](#) [2: Device encryption in Windows - Microsoft Support](#) [3: Can You Turn on BitLocker on Windows 10 Home?](#) [4: How to enable device encryption on Windows 10 Home](#)

---

### Question: 230

---

Which of the following combinations meets the requirements for mobile device multifactor authentication?

- A . Password and PIN
- B . Password and swipe
- C . Fingerprint and password
- D . Swipe and PIN

---

**Answer: C**

---

Explanation:

[Mobile device multifactor authentication \(MFA\) is a method of verifying a user's identity by requiring two or more factors, such as something the user knows \(e.g., password, PIN, security question\), something the user has \(e.g., smartphone, OTP app, security key\), or something the user is \(e.g., fingerprint, face, iris\)](#)<sup>12</sup>. The combination of fingerprint and password meets the requirements for mobile device MFA because it uses two different factors:

[something the user is \(fingerprint\) and something the user knows \(password\). The other combinations do not meet the requirements because they use only one factor: something the user knows \(password or PIN\) or something the user does \(swipe\).](#)

[Reference 1: Set up the Microsoft Authenticator app as your verification method](#) [2: What is Multi-Factor Authentication \(MFA\)? | OneLogin](#)

---

### **Question: 231**

---

Which of the following should be documented to ensure that the change management plan is followed?

- A . Scope of the change
- B . Purpose of the change
- C . Change rollback plan
- D . Change risk analysis

---

**Answer: A**

---

Explanation:

The scope of the change is one of the elements that should be documented to ensure that the change management plan is followed. The scope of the change defines the boundaries and limitations of the change, such as what is included and excluded, what are the deliverables and outcomes, what are the assumptions and constraints, and what are the dependencies and risks. The scope of the change helps to clarify the expectations and objectives of the change, as well as to prevent scope creep or deviation from the original plan. The scope of the change also helps to measure the progress and success of the change, as well as to communicate the change to the stakeholders and the team.

---

### **Question: 232**

---

A Windows computer is experiencing slow performance when the user tries to open programs and files. The user recently installed a new software program from an external website.

Various websites are being redirected to an unauthorized site, and Task Manager shows the CPU usage is consistently at 100%. Which of the following should the technician do first?

- A . Uninstall the new program.
- B . Check the HOSTS file.
- C . Restore from a previous backup.
- D . Clear the web browser cache.

---

**Answer: A**

---

Explanation:

The symptoms that the user's Windows computer is experiencing suggest that the new software program that the user installed from an external website may be malicious or incompatible with the system. The program may be consuming a lot of CPU resources, slowing down the performance of other programs and files. The program may also be altering the browser settings or the HOSTS file, causing the web redirection to an unauthorized site. The first step that the technician should do is to uninstall the new program from the Control Panel or the Settings app, and then restart the computer. This may resolve the issue and restore the normal functionality of the computer. If the problem persists, the technician may need to perform additional steps, such as scanning for malware, checking the HOSTS file, clearing the web browser cache, or restoring from a previous backup

---

### **Question: 233**

---

A user's iPhone was permanently locked after several failed log-in attempts. Which of the following authentication methods are needed to restore access, applications, and data to the device?

- A . Fingerprint and pattern
- B . Facial recognition and PIN code
- C . Primary account and password
- D . Recovery contact and recovery key

---

**Answer: D**

---

Explanation:

If a user's iPhone is permanently locked after several failed log-in attempts, the user will need to use the recovery contact and recovery key to restore access, applications, and data to the device. The recovery contact is a trusted person who can receive a verification code from Apple and share it with the user. The recovery key is a 28-character code that the user created when setting up two-factor authentication for their Apple ID. The user will need to enter both the verification code and the recovery key on another device or computer to unlock their iPhone. This method will erase the iPhone and restore it from the iCloud backup

---

### **Question: 234**

---

A user clicks a link in an email. A warning message in the user's browser states the site's certificate cannot be verified. Which of the following is the most appropriate action for a technician to take?

- A . Click proceed.
- B . Report the employee to the human resources department for violating company policy.
- C . Restore the computer from the last known backup.
- D . Close the browser window and report the email to IT security.

---

**Answer: D**

---

Explanation:

A warning message in the user's browser stating the site's certificate cannot be verified indicates that the site may be insecure, fraudulent, or malicious. This could be a sign of a phishing attempt, where the sender of the email tries to trick the user into clicking a link that leads to a fake website that mimics a legitimate one, in order to steal the user's personal or financial information. The most appropriate action for a technician to take in this situation is to close the browser window and report the email to IT security, who can investigate the source and content of the email, and take the necessary steps to protect the user and the network from potential harm. Clicking proceed could expose the user to malware, identity theft, or data breach. Reporting the employee to the human resources department for violating company policy is unnecessary and harsh, as the user may not have been aware of the phishing attempt or the company policy. Restoring the computer from the last known backup is premature and ineffective, as the user may not have been infected by anything, and the backup may not remove the email or the link from the user's inbox

---

### **Question: 235**

---

A laptop that was in the evidence room of a police station is missing. Which of the following is the best reason to refer to chain of custody documentation?

- A . To determine which party had the machine and when.
- B . To remotely wipe sensitive data from the machine.
- C . To gather the information needed to replace the machine.
- D . To alert the owner that the password needs to be changed.

---

**Answer: A**

---

Explanation:

Chain of custody documentation is a record of the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. It is important to maintain a chain of custody to ensure the integrity and authenticity of the evidence, and to prevent tampering or contamination. If a laptop that was in the evidence room of a police station is missing, the best reason to refer to chain of custody documentation is to determine which party had the machine and when. This can help to identify the possible suspects, locate the missing laptop, and verify if the evidence on the laptop was compromised or not

---

### **Question: 236**

---

A help desk technician needs to remotely access and control a customer's Windows PC by using a secure session that allows the technician the same control as the customer. Which of the following tools provides this type of access?

- A . FTP
- B . RDP
- C . SSH
- D . VNC

---

**Answer: B**

---

Explanation:

RDP stands for Remote Desktop Protocol, which is a proprietary protocol developed by Microsoft that allows a user to remotely access and control another computer over a network. RDP provides a secure session that encrypts the data between the client and the host, and allows the user to see and interact with the desktop and applications of the remote computer as if they were sitting in front of it. RDP also supports features such as audio, video, clipboard, printer, and file sharing, as well as multiple monitor support and session recording. To use RDP, the host computer must have Remote Desktop enabled and configured, and the client computer must have a Remote Desktop client software installed. The client can connect to the host by entering its IP address, hostname, or domain name, and providing the login credentials of a user account on the host. RDP is commonly used for remote administration, technical support, and remote work scenarios

---

### **Question: 237**

---

Which of the following file extensions should a technician use for a PowerShell script?

- A .ps1
- B .py
- C .sh
- D .bat
- E .cmd

---

**Answer: A**

---

Explanation:

A PowerShell script is a plain text file that contains one or more PowerShell commands. Scripts have a .ps1 file extension and can be run on your computer or in a remote session. PowerShell scripts can be used to automate tasks and change settings on Windows devices. To create and run a PowerShell script, you need a text editor (such as Visual Studio Code or Notepad) and the PowerShell Integrated Scripting Environment (ISE) console. You also need to enable the correct execution policy to allow scripts to run on your system

---

### **Question: 238**

---

Which of the following operating systems is most commonly used in embedded systems?

- A . Chrome OS
- B . macOS
- C . Windows
- D . Linux

---

**Answer: D**

---

Explanation:

Linux is the most commonly used operating system in embedded systems because it is open source, free, customizable, and supports a wide range of architectures and devices. Linux also offers many advantages for

embedded development, such as real-time capabilities, modularity, security, scalability, and reliability. Linux can run on embedded systems with limited resources, such as memory, storage, or power, and can be tailored to the specific needs of the application. Linux also has a large and active community of developers and users who contribute to its improvement and innovation. Some examples of embedded systems that use Linux are smart TVs, routers, drones, robots, smart watches, and IoT devices

---

### Question: 239

---

A customer installed a new web browser from an unsolicited USB drive that the customer received in the mail. The browser is not working as expected, and internet searches are redirected to another site. Which of the following should the user do next after uninstalling the browser?

- A . Delete the browser cookies and history.
- B . Reset all browser settings.
- C . Change the browser default search engine.
- D . Install a trusted browser.

---

**Answer: D**

---

Explanation:

The customer's web browser is likely infected by a browser hijacker, which is a type of malware that changes the browser's settings and redirects the user to malicious websites. A browser hijacker can also steal the user's personal data, display unwanted ads, and install more malware on the device. To remove a browser hijacker, the user should first uninstall the browser from the Control Panel, then scan the device with an antivirus or anti-malware program, and finally install a trusted browser from a legitimate source. Deleting the browser cookies and history, resetting the browser settings, or changing the browser default search engine may not be enough to get rid of the browser hijacker, as it may have embedded itself into the system or other browser components.

---

### Question: 240

---

A technician has identified malicious traffic originating from a user's computer. Which of the following is the best way to identify the source of the attack?

- A . Investigate the firewall logs.
- B . Isolate the machine from the network.
- C . Inspect the Windows Event Viewer.
- D . Take a physical inventory of the device.

---

**Answer: B**

---

Explanation:

Isolating the machine from the network is the best way to identify the source of the attack, because it prevents the malicious traffic from spreading to other devices or reaching the attacker. Isolating the machine can also help

preserve the evidence of the attack, such as the malware files, the network connections, the registry entries, or the system logs. By isolating the machine, a technician can safely analyze the machine and determine the source of the attack, such as a phishing email, a compromised website, a removable media, or a network vulnerability.

---

### **Question: 241**

---

A user's computer unexpectedly shut down immediately after the user plugged in a USB headset. Once the user turned the computer back on, everything was functioning properly, including the headset. Which of the following Microsoft tools would most likely be used to determine the root cause?

- A . Event Viewer
- B . System Configuration
- C . Device Manager
- D . Performance Monitor

---

**Answer: A**

---

Explanation:

Event Viewer is a Microsoft tool that records and displays system events, errors, warnings, and information. Event Viewer can help troubleshoot and diagnose problems, such as unexpected shutdowns, by showing the details of what happened before, during, and after the incident. Event Viewer can also show the source of the event, such as an application, a service, a driver, or a hardware device. By using Event Viewer, a technician can identify the root cause of the unexpected shutdown, such as a power failure, a thermal event, a driver conflict, or a malware infection.

---

### **Question: 242**

---

A technician is troubleshooting a PC because the user has reported strange pop-up windows and computer performance issues. Which of the following actions should the technician take next?

- A . Isolate the machine from the network.
- B . Scan the system for hidden files.
- C . Disable unused ports.
- D . Install antivirus software.
- E . Reconfigure the firewall.

---

**Answer: A**

---

Explanation:

Isolating the machine from the network is a good practice when troubleshooting a PC that is suspected of being infected with malware. This can prevent the malware from spreading to other devices on the network or communicating with external servers that may control or exploit the malware. Isolating the machine can be done by disconnecting the network cable, disabling the wireless adapter, or blocking the network traffic with a firewall.

---

### **Question: 243**

---

A technician is modifying the default home page of all the workstations in a company. Which of the following will help to implement this change?

- A . Group Policy
- B . Browser extension
- C . System Configuration
- D . Task Scheduler

---

**Answer: A**

---

Explanation:

Group Policy is a feature of Windows that allows administrators to centrally manage and configure the settings of computers and users in a domain network. Group Policy can be used to modify the default home page of all the workstations in a company by creating and applying a policy that specifies the desired URL for the home page. This way, the change will be automatically applied to all the workstations that are joined to the domain and receive the policy.

---

### **Question: 244**

---

Which of the following environments allows for the testing of critical systems without the risk of them being negatively impacted by changes?

- A . Regression
- B . Cloud
- C . Production
- D . Sandbox

---

**Answer: D**

---

Explanation:

A sandbox is an isolated environment that allows for the testing of critical systems without the risk of them being negatively impacted by changes. A sandbox can be used to simulate real-world scenarios, experiment with new features, debug errors, or evaluate the performance and security of a system. A sandbox can be created using virtualization, emulation, or containerization technologies. A sandbox prevents any changes made in the testing environment from affecting the production environment, which is the actual system that is used by the end users.

---

## **Question: 245**

---

Remote employees need access to information that is hosted on local servers at the company. The IT department needs to find a solution that gives employees secure access to the company's resources as if the employees were on premises. Which of the following remote connection services should the IT team

implement?

- A . SSH
- B . VNC
- C . VPN
- D . RDP

---

**Answer: C**

---

Explanation:

A VPN (Virtual Private Network) is a service that allows remote employees to access the company's network resources securely over the internet as if they were on premises. A VPN encrypts the data traffic between the employee's device and the VPN server, and assigns the employee a virtual IP address that belongs to the company's network. This way, the employee can access the local servers, files, printers, and other resources without exposing them to the public internet. A VPN also protects the employee's privacy and identity by masking their real IP address and location.

---

## **Question: 246**

---

A technician wants to install Developer Mode on a Windows laptop but is receiving a 'failed to install package' message. Which of the following should the technician do first?

- A . Ensure internet connectivity.
- B . Check for Windows updates.
- C . Enable SSH.
- D . Reboot computer.

---

**Answer: A**

---

Explanation:

Developer Mode on Windows 10 is a feature that allows developers to test and debug their applications on their devices, as well as sideload apps and access other developer tools<sup>12</sup>. To enable Developer Mode, the user needs to go to the Settings app, select Update & Security, choose For Developers, and switch to Developer Mode<sup>123</sup>. However, enabling Developer Mode requires internet connectivity, as Windows will download and install a package of features, such as Windows Device Portal and SSH services, that are necessary for Developer Mode<sup>124</sup>. If the user does not have internet connectivity, they will receive a "failed to install package" message when trying to enable Developer Mode<sup>4</sup>. Therefore, the first thing that the technician should do is to ensure that the laptop has internet access, either through Wi-Fi or Ethernet, and then try to enable Developer Mode again<sup>4</sup>.

---

## **Question: 247**

---

After a security event, a technician removes malware from an affected laptop and disconnects the laptop from the network. Which of the following should the technician do to prevent the operating system from automatically returning to an infected state?

- A . Enable System Restore.
- B . Disable System Restore.
- C . Enable antivirus.
- D . Disable antivirus.
- E . Educate the user.

---

**Answer: B**

---

Explanation:

System Restore is a feature that allows the user to revert the system to a previous state. However, this can also restore the malware that was removed by the technician. Disabling System Restore can prevent the operating system from automatically returning to an infected state. Enabling antivirus, educating the user, and enabling System Restore are good preventive measures, but they do not address the question. Disabling antivirus can make the system more vulnerable to malware attacks

---

## **Question: 248**

---

A user is trying to use proprietary software, but it crashes intermittently. The user notices that the desktop is displaying a 'low memory' warning message. Upon restarting the desktop, the issue persists. Which of the following should a technician do next to troubleshoot the issue?

- A . Reimage the computer.
- B . Replace the system RAM.
- C . Reinstall and update the failing software.
- D . Decrease the page file size.

---

**Answer: C**

---

Explanation:

The most likely cause of the intermittent crashes is that the proprietary software is incompatible, outdated, or corrupted. Reinstalling and updating the software can fix these issues and ensure the software runs smoothly. Reimaging the computer or replacing the system RAM are too drastic and unnecessary steps. Decreasing the page file size can worsen the low memory problem and affect the performance of other applications.

---

### **Question: 249**

---

A technician needs to reimage a desktop in an area without network access. Which of the following should the technician use? (Select two).

- A . USB
- B . PXE
- C . Optical media
- D . Partition
- E . Boot record
- F . SMB

---

**Answer: A, C**

---

Explanation:

A technician needs to reimage a desktop in an area without network access, which means that the technician cannot use network-based methods such as PXE or SMB to deploy the image. Therefore, the technician should use offline methods that involve removable media such as USB or optical media. USB and optical media are common ways to store and transfer system images, and they can be used to boot the desktop and initiate the reimaging process. The technician will need to create a bootable USB or optical media that contains the system image and the imaging software, and then insert it into the desktop and change the boot order in the BIOS or UEFI settings. The technician can then follow the instructions on the screen to reimage the desktop.

---

### **Question: 250**

---

A user reports a hardware issue to the help desk. Which of the following should the help desk technician do first when responding to the user?

- A . Ask the user for the model number of the hardware.
- B . Offer a temporary replacement device to the user.
- C . Submit the issue to the manufacturer.
- D . Remotely install updates to the device driver.

---

**Answer: A**

---

Explanation:

The first step in troubleshooting a hardware issue is to identify the hardware device that is causing the problem. Asking the user for the model number of the hardware can help the help desk technician to find the specifications, manuals, drivers, and other relevant information for the device. This can also help the technician to determine if the device is compatible with the user's system, if it has any known issues or defects, and if it is covered by warranty or support contract. Asking the user for the model number of the hardware is a help desk best practice that can save time and effort in resolving the issue.

---

### **Question: 251**

---

A remote user contacts the help desk about an email that appears to be distorted. The technician is unsure what the user means and needs to view the email to assist with troubleshooting. Which of the following should the technician use to assist the user?

- A . VNC
- B . SSH
- C . VPN
- D . RMM

---

**Answer: D**

---

Explanation:

The best tool to use to assist the user with viewing the email is RMM, which stands for remote monitoring and management. This is a software that allows the technician to remotely access, monitor, and manage the user's computer and applications. The technician can use RMM to view the user's screen, control the mouse and keyboard, and troubleshoot the email issue. The other tools are not suitable for this task. VNC is a software that allows remote desktop sharing, but it requires the user to install and configure it on their computer, which may not be feasible or convenient. SSH is a protocol that allows secure remote access to a command-line interface, but it is not useful for viewing graphical applications such as email. VPN is a technology that creates a secure and encrypted connection over a public network, but it does not provide remote access or control of the user's computer.

---

### **Question: 252**

---

A technician is creating a location on a Windows workstation for a customer to store meeting minutes. Which of the following commands should the technician use?

- A . c: \minutes
- B . dir
- C . rmdir
- D . md

---

**Answer: D**

---

Explanation:

The command `md` stands for make directory and is used to create a new directory or folder in the current location. In this case, the technician can use `md minutes` to create a folder named `minutes` in the `C:` drive. The other commands are not relevant for this task. `c: \minutes` is not a command but a path to a folder. `dir` is used to display a list of files and folders in the current directory. `rmdir` is used to remove or delete an existing directory or folder.

---

### **Question: 253**

---

Which of the following is the most likely to use NTFS as the native filesystem?

- A . macOS
- B . Linux
- C . Windows
- D . Android

---

**Answer: C**

---

Explanation:

NTFS stands for New Technology File System, which is a proprietary file system developed by Microsoft<sup>4</sup>. NTFS is the default file system for the Windows NT family of operating systems, which includes Windows 10, Windows Server 2019, and other versions<sup>5</sup>. NTFS provides features such as security, encryption, compression, journaling, and large volume support<sup>45</sup>. NTFS is not the native file system for other operating systems, such as macOS, Linux, or Android, although some of them can read or write to NTFS volumes with third-party drivers or tools

---

### **Question: 254**

---

Which of the following involves sending arbitrary characters in a web page request?

- A . SMS
- B . SSL
- C . XSS
- D . VPN

---

**Answer: C**

---

Explanation:

XSS stands for cross-site scripting, which is a web security vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users<sup>1</sup>. XSS involves sending arbitrary characters in a web page request, such as a query string, a form field, a cookie, or a header, that contain a malicious script. The web server does not validate or encode the input, and returns it as part of the web page response. The browser then executes the script, which can perform various actions on behalf of the attacker, such as stealing cookies, session tokens, or other sensitive information, redirecting the user to a malicious site, or displaying fake content

---

### **Question: 255**

---

A user's application is unresponsive. Which of the following Task Manager tabs will allow the user to address the situation?

- A . Startup
- B . Performance
- C . Application history

## D . Processes

---

**Answer: D**

---

Explanation:

The Processes tab in the Task Manager shows all the running processes on the computer, including applications and background services. The user can use this tab to identify the unresponsive application and end its process by right-clicking on it and selecting End task. This will free up the system resources and close the application. The other tabs in the Task Manager do not allow the user to address the situation. The Startup tab shows the programs that run when the computer starts, the Performance tab shows the system resource usage and statistics, and the Application history tab shows the resource usage of the applications over time

---

### **Question: 256**

---

Which of the following is the most likely reason a filtration system is critical for data centers?

- A . Plastics degrade over time.
- B . High humidity levels can rust metal.
- C . Insects can invade the data center.
- D . Dust particles can clog the machines.

---

**Answer: B**

---

Explanation:

A filtration system is critical for data centers because it can control the humidity and temperature levels in the environment. High humidity levels can cause condensation and corrosion on the metal components of the servers and other equipment, leading to malfunction and damage. A filtration system can also prevent dust, dirt, and other contaminants from entering the data center and clogging the machines or causing overheating.

---

### **Question: 257**

---

A technician has verified a computer is infected with malware. The technician isolates the system and updates the anti-malware software. Which of the following should the technician do next?

- A . Run one scan and schedule future scans.
- B . Back up the uninfected files and reimage the computer.
- C . Restore the clean backup copies of the infected files.
- D . Run repeated remediation scans until the malware is removed.

---

**Answer: D**

---

Explanation:

Malware is malicious software that can cause damage or harm to a computer system or network<sup>4</sup>. A technician has verified a computer is infected with malware by observing unusual behavior, such as slow performance, pop-ups, or unwanted ads. The technician isolates the system and updates the anti-malware software to prevent further infection or spread of the malware. The next step is to run repeated remediation scans until the malware is removed. A remediation scan is a scan that detects and removes malware from the system. Running one scan may not be enough to remove all traces of malware, as some malware may hide or regenerate itself.

---

### **Question: 258**

---

A technician needs to track evidence for a forensic investigation on a Windows computer. Which of the following describes this process?

- A . Valid license
- B . Data retention requirements
- C . Material safety data sheet
- D . Chain of custody

---

**Answer: D**

---

---

### **Question: 259**

---

When trying to access a secure internal network, the user receives an error messaging stating, 'There is a problem with this website's security certificate.' The user reboots the desktop and tries to access the website again, but the issue persists. Which of the following should the user do to prevent this error from reoccurring?

- A . Reimage the system and install SSL.
- B . Install Trusted Root Certificate.
- C . Select View Certificates and then Install Certificate.
- D . Continue to access the website.

---

**Answer: C**

---

Explanation:

The error message indicates that the website's security certificate is not trusted by the user's device, which may prevent the user from accessing the secure internal network. To resolve this issue, the user can view the certificate details and install it on the device, which will add it to the trusted root certificate store. Reimaging the system and installing SSL, installing Trusted Root Certificate, or continuing to access the website are not recommended solutions, as they may compromise the security of the device or the network.

---

### **Question: 260**

---

Malware is installed on a device after a user clicks on a link in a suspicious email. Which of the following is the best way to remove the malware?

- A . Run System Restore.
- B . Place in recovery mode.
- C . Schedule a scan.
- D . Restart the PC.

---

**Answer: B**

---

Explanation:

Recovery mode is a special boot option that allows the user to access advanced tools and features to troubleshoot and remove malware from the device. Recovery mode can also restore the system to a previous state or reset the device to factory settings. Running System Restore, scheduling a scan, or restarting the PC may not be effective in removing the malware, as it may still be active or hidden in the system files.

---

### **Question: 261**

---

A technician needs to replace a PC's motherboard. The technician shuts down the PC. Which of the following steps should the technician take next?

- A . Turn off the monitor.
- B . Remove the power cord.
- C . Remove the PSU.
- D . Remove the RAM modules.

---

**Answer: B**

---

Explanation:

Removing the power cord is the first step to ensure the safety of the technician and the PC components. This will prevent any electrical shock or damage that may occur if the PC is still connected to a power source. The technician should also press the power button to drain any residual power from the capacitors.

---

### **Question: 262**

---

A technician is unable to completely start up a system. The OS freezes when the desktop background appears, and the issue persists when the system is restarted. Which of the following should the technician do next to troubleshoot the issue?

- A . Disable applicable BIOS options.
- B . Load the system in safe mode.
- C . Start up using a flash drive OS and run System Repair.
- D . Enable Secure Boot and reinstall the system.

---

**Answer: B**

---

## Explanation:

Loading the system in safe mode is a common troubleshooting step that allows the technician to isolate the problem by disabling unnecessary drivers and services. This can help determine if the issue is caused by a faulty device, a corrupted system file, or a malware infection.

---

### Question: 263

---

In an organization with a standardized set of installed software, a developer submits a request to have new software installed. The company does not currently have a license for this software, but the developer already downloaded the installation file and is requesting that the technician install it. The developer states that the management team approved the business use of this software. Which of the following is the best action for the technician to take?

- A . Contact the software vendor to obtain the license for the user, and assist the user with installation once the license is purchased.
- B . Run a scan on the downloaded installation file to confirm that it is free of malicious software, install the software, and document the software installation process.
- C . Indicate to the developer that formal approval is needed; then, the IT team should investigate the software and the impact it will have on the organization before installing the software.
- D . Install the software and run a full system scan with antivirus software to confirm that the operating system is free of malicious software.

---

## Answer: C

---

## Explanation:

Installing new software on an organization's system or device can have various implications, such as compatibility, security, performance, licensing, and compliance issues. Therefore, it is important to follow the best practices for software installation, such as doing research on the software, checking the system requirements, scanning the installation file for malware, and obtaining the proper license<sup>345</sup>. The technician should not install the software without formal approval from the management team, as this could violate the organization's policies or regulations. The technician should also not install the software without investigating the software and its impact on the organization, as this could introduce potential risks or problems to the system or device. The technician should indicate to the developer that formal approval is needed, and then work with the IT team to evaluate the software and its suitability for the organization before installing it

---

### Question: 264

---

Which of the following does MFA provide?

- A . Security enhancement
- B . Encryption
- C . Digital signature
- D . Public key infrastructure

---

**Answer: A**

---

Explanation:

MFA stands for multi-factor authentication, which is an electronic authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN1. MFA provides security enhancement by making it harder for attackers to compromise the user's identity or credentials, as they would need to obtain more than just the username and password.MFA can also prevent unauthorized access to sensitive data or resources, as well as reduce the risk of identity theft or fraud2.

---

### **Question: 265**

---

A user is setting up a new Windows 10 laptop. Which of the following Windows settings should be used to input the SSID and password?

- A . Network & Internet
- B . System
- C . Personalization
- D . Accounts

---

**Answer: A**

---

Explanation:

The Network & Internet settings in Windows 10 allow the user to input the SSID and password of a Wi-Fi network, as well as manage other network-related options, such as airplane mode, mobile hotspot, VPN, proxy, etc1.To access the Network & Internet settings, the user can select the Start button, then select Settings > Network & Internet2.Alternatively, the user can right-click the Wi-Fi icon on the taskbar and click 'Open Network & Internet Settings'3.

The System settings in Windows 10 allow the user to configure the display, sound, notifications, power, storage, and other system-related options1.The Personalization settings in Windows 10 allow the user to customize the background, colors, lock screen, themes, fonts, and other appearance-related options1.The Accounts settings in Windows 10 allow the user to manage the user accounts, sign-in options, sync settings, and other account-related options1. None of these settings can be used to input the SSID and password of a Wi-Fi network.

The Official CompTIA A+ Core 2 Study Guide1, page 221, 222, 223, 224.

---

### **Question: 266**

---

Applications on a computer are not updating, which is preventing the user from opening certain files. Which of the following MMC snap-ins should the technician launch next to continue troubleshooting the issue?

- A . gpedit.msc

- B . perfmon.msc
- C . devmgmt.msc

---

Answer: C

---

Explanation:

devmgmt.msc is the MMC snap-in that opens the Device Manager, a tool that allows the technician to view and manage the hardware devices and their drivers on the computer1. If the applications are not updating properly, it could be due to outdated, corrupted, or incompatible drivers that prevent the hardware from functioning normally. The technician can use the Device Manager to update, uninstall, rollback, or disable the drivers, as well as scan for hardware changes, troubleshoot problems, and view device properties2.

gpedit.msc is the MMC snap-in that opens the Group Policy Editor, a tool that allows the technician to configure the local or domain group policy settings for the computer or a group of computers3. Group policy settings can affect the security, performance, and functionality of the system, but they are not directly related to the application updates or the hardware drivers.

perfmon.msc is the MMC snap-in that opens the Performance Monitor, a tool that allows the technician to monitor and analyze the performance of the system and its components, such as processor, memory, disk, network, etc4. Performance Monitor can display real-time data or collect log data for later analysis, as well as generate reports and alerts based on the performance counters5. Performance Monitor can help the technician identify and diagnose performance issues, but it does not provide a way to manage the hardware drivers.

The Official CompTIA A+ Core 2 Study Guide6, page 223, 225, 227, 228.

---

### Question: 267

---

A technician wants to mitigate unauthorized data access if a computer is lost or stolen. Which of the following features should the technician enable?

- A . Network share
- B . Group Policy
- C . BitLocker
- D . Static IP

---

Answer: C

---

Explanation:

BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices1. BitLocker helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protected devices are decommissioned or recycled1. Network share, Group Policy, and Static IP are not features that can prevent unauthorized data access if a computer is lost or stolen.

---

### Question: 268

---

Which of the following protocols supports fast roaming between networks?

- A . WEP
- B . WPA
- C . WPA2
- D . LEAP
- E . PEAP

---

**Answer: B**

---

Explanation:

[WPA2 is the only protocol among the options that supports fast roaming between networks. Fast roaming, also known as IEEE 802.11r or Fast BSS Transition \(FT\), enables a client device to roam quickly in environments implementing WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another1. WEP, WPA, LEAP, and PEAP do not support fast roaming and require the client device to perform the full authentication process every time it roams, which can cause delays and interruptions in the network service.](#)

---

### Question: 269

---

A user's company phone was stolen. Which of the following should a technician do next?

- A . Perform a low-level format.
- B . Remotely wipe the device.
- C . Degauss the device.
- D . Provide the GPS location of the device.

---

**Answer: B**

---

Explanation:

Remotely wiping the device is the best option to prevent unauthorized access to the company data stored on the phone. A low-level format, degaussing, or providing the GPS location of the device are not feasible or effective actions to take in this scenario.

---

## **Question: 270**

---

A user's antivirus software reports an infection that it is unable to remove. Which of the following is the most appropriate way to remediate the issue?

- A . Disable System Restore.
- B . Utilize a Linux live disc.
- C . Quarantine the infected system.
- D . Update the anti-malware.

---

**Answer: C**

---

Explanation:

Quarantining the infected system is the most appropriate way to remediate the issue of an infection that the antivirus software cannot remove. Quarantining means isolating the system from the network and other devices to prevent the infection from spreading or causing further damage. Quarantining also allows the technician to perform further analysis and removal of the infection without risking the security of other systems or data.

Some of the steps involved in quarantining an infected system are:

Disconnect the system from the internet and any local network connections, such as Wi-Fi, Ethernet, Bluetooth, or USB.

Disable any file-sharing or remote access services on the system, such as Windows File Sharing, Remote Desktop, or TeamViewer.

Use a separate device to download and update the antivirus software and any other tools that may be needed to remove the infection, such as malware scanners, rootkit removers, or bootable rescue disks.

Transfer the updated antivirus software and tools to the infected system using a removable media, such as a CD, DVD, or USB flash drive. Scan the removable media for any infections before and after using it on the infected system.

Run the antivirus software and tools on the infected system and follow the instructions to delete or quarantine the infection. If the infection is persistent or complex, it may require booting the system from a rescue disk or using a Linux live disc to access and clean the system files.

After the infection is removed, restore the system to a previous clean state using System Restore, backup, or recovery partition. Scan the system again to ensure that it is clean and secure. Reconnect the system to the network and update the system and the antivirus software.

[How to Identify and Repair Malware or Virus Infected Computers, section 31](#)

[Uninstalling Antivirus Software, the Clean Way: 40 Removal Tools & Instructions, section 22](#)

[How to manually remove an infected file from a Windows computer3](#)

[The Official CompTIA A+ Core 2 Study Guide \(220-1102\), page 2194](#)

---

## **Question: 271**

---

A technician cannot uninstall a system driver because the driver is currently in use. Which of the following tools should the technician use to help uninstall the driver?

- A . msinfo32.exe
- B . dxdiag.exe
- C . msconfig.exe
- D . regedit.exe

---

**Answer: C**

---

Explanation:

The msconfig.exe tool, also known as the System Configuration utility, is a tool that allows users to modify various system settings, such as startup options, services, boot options, and more. One of the features of msconfig.exe is the ability to disable or enable device drivers that are loaded during the system startup. By using msconfig.exe, a technician can prevent a driver from being loaded and used by the system, which will allow them to uninstall it without any errors. To use msconfig.exe to disable a driver, the technician can follow these steps:

Open the Run dialog box by pressing the Windows key + R.

Type msconfig.exe and press Enter.

Click on the Boot tab and then click on Advanced options.

Check the box next to No GUI boot and click OK. This will prevent the graphical user interface from loading during the boot process, which will also prevent some drivers from loading.

Click on the Services tab and check the box next to Hide all Microsoft services. This will show only the third-party services and drivers that are running on the system.

Find the service or driver that corresponds to the device that the technician wants to uninstall and uncheck the box next to it. This will disable the service or driver from starting during the system startup.

Click Apply and OK and then restart the computer.

After the computer restarts, the technician can use the Device Manager or the Control Panel to uninstall the driver that was previously in use.

[How to Completely Remove/Uninstall a Driver in Windows, section 31](#)

[The Official CompTIA A+ Core 2 Study Guide \(220-1102\), page 2212](#)

---

## **Question: 272**

---

A technician has verified that a user's computer has a virus and the antivirus software is out of date. Which of the following steps should the technician take next?

- A . Quarantine the computer.

- B . Use a previous restore point.
- C . Educate the end user about viruses.
- D . Download the latest virus definitions.

---

**Answer: D**

---

Explanation:

The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer. Therefore, the technician should download the latest virus definitions from the antivirus vendor's website or use the update feature in the antivirus program before scanning the computer for viruses.

[How to remove malware or viruses from my Windows 10 PC, section 21](#)

[How to Remove a Virus From a Computer in 2023, section 32](#)

[The Official CompTIA A+ Core 2 Study Guide \(220-1102\), page 2193](#)

---

### **Question: 273**

---

A user receives a call from someone claiming to be a technical support agent. The caller asks the user to log in to the computer.

Which of the following security measures should the user take to ensure security and privacy?

- A . Only accept calls from known people.
- B . Disregard any suspicious emails.
- C . Update the antivirus software.
- D . Enable two-factor authentication.
- E . Install a malware scanner.

---

**Answer: A**

---

Explanation:

This is a scenario of a potential tech support scam, where a fraudster pretends to be a technical support agent and tries to trick the user into giving them access to the computer, personal information, or money. The user should not trust any unsolicited calls from unknown people claiming to be from tech support, as they might be trying to install malware, steal data, or charge for fake services. The user should only accept calls from known people, such as their IT department, their service provider, or their software vendor, and verify their identity before logging in to the computer. The user should also report any suspicious calls to the appropriate authorities or organizations.

[How to protect against tech support scams1](#)

[Avoid and report Microsoft technical support scams2](#)

[How to Protect Against Technical Support Scams3](#)

[How To Recognize and Avoid Tech Support Scams4](#)

---

### **Question: 274**

---

A technician is moving a Windows workstation from the accounting department to the sales department and needs to update the IP and gateway settings. Which of the following Control Panel utilities should the technician use?

- A . Programs and Features
- B . Network and Sharing Center
- C . User Accounts
- D . Device Manager

---

**Answer: B**

---

Explanation:

The Network and Sharing Center is a Control Panel utility that allows users to view and modify network settings, such as IP address, subnet mask, default gateway, DNS servers, and network profiles. To change the IP and gateway settings of a Windows workstation, the technician can follow these steps:

Open the Network and Sharing Center by clicking on the network icon in the system tray or by searching for it in the Start menu.

Click on Change adapter settings on the left sidebar.

Right-click on the network adapter that is connected to the network and select Properties.

Double-click on Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6) depending on the network protocol used.

Select Use the following IP address and enter the desired IP address, subnet mask, and default gateway for the workstation. Alternatively, select Obtain an IP address automatically if the network uses DHCP to assign IP addresses dynamically.

Click OK to save the changes and close the dialog boxes.

[The Official CompTIA A+ Core 2 Study Guide \(220-1102\), page 2171](#)

[How to change the IP address in Windows 10 and Windows 11 \(4 ways\), section 12](#)

---

### **Question: 275**

---

A technician is familiar with most personnel at a customer's location and has clearance to work unsupervised. Which of the following describes how the technician should handle personal communication while on site?

- A . Respond to calls and text messages while on site but not when working directly with personnel.
- B . Respond to calls and text messages only from family.
- C . Respond to calls and text messages only when an emergency situation requires a response.
- D . Respond to calls and text messages discreetly while on site.

---

**Answer: C**

---

Explanation:

A technician should handle personal communication while on site in a professional and respectful manner. According to the CompTIA A+ Core 2 (220-1102) exam objectives, one of the best practices for communication skills is to "avoid distractions and interruptions" when working with customers<sup>1</sup>. This means that the technician should not respond to calls and text messages that are not related to the work or the customer, unless there is an emergency situation that requires a response. Responding to personal communication while on site can be seen as rude, unprofessional, and disrespectful to the customer and their time. It can also affect the quality and efficiency of the technician's work and cause errors or delays. Therefore, the technician should only respond to calls and text messages when an emergency situation requires a response, and inform the customer about the situation and apologize for the interruption.

The other options are not appropriate for handling personal communication while on site. Responding to calls and text messages while on site but not when working directly with personnel (A) is still distracting and unprofessional, as it can interfere with the technician's focus and productivity. Responding to calls and text messages only from family (B) is not a valid criterion, as the technician may receive calls and text messages from other sources that are not related to the work or the customer. Responding to calls and text messages discreetly while on site (D) is not a good practice, as it can still be noticed by the customer or other personnel and create a negative impression.

---

[1:CompTIA A+ Certification Exam Core 2 Objectives - CompTIA](#)

---

### **Question: 276**

---

A technician is trying to connect to a user's laptop in order to securely install updates. Given the following information about the laptop:

Hostname:	corp-laptop-222
IP Address:	192.168.0.45
Gateway:	192.168.1.1
Subnet Mask:	255.255.252.0
Open Ports:	21, 22, 80, 443

Which of the following should the technician do to connect via RDP?

- A . Confirm the user can ping the default gateway.
- B . Change the IP address on the user's laptop.
- C . Change the subnet mask on the user's laptop.
- D . Open port 3389 on the Windows firewall.

---

**Answer: D**

---

Explanation:

In order to connect to a user's laptop via RDP, the technician should open port 3389 on the Windows firewall. This is because RDP uses port 3389 for communication12. The other options are not necessary or relevant for establishing an RDP connection.

Confirming the user can ping the default gateway is not required for RDP, as it only tests the network connectivity between the user's laptop and the router. RDP works over the internet, so the technician should be able to ping the user's laptop directly using its IP address3.

Changing the IP address on the user's laptop is not needed for RDP, as long as the IP address is valid and not conflicting with another device on the network. The user's laptop has a valid IP address of 192.168.0.45, which belongs to the same subnet as the gateway (192.168.0.1) and the subnet mask (255.255.255.0)4.

Changing the subnet mask on the user's laptop is not required for RDP, as long as the subnet mask matches the network configuration. The user's laptop has a correct subnet mask of 255.255.255.0, which defines a network with 254 possible hosts4.

1: [What is RDP and How Does It Work?- CompTIA]2:CompTIA A+ Certification Exam Core 2 Objectives - CompTIA3: [Ping (networking utility) - Wikipedia]4: [IP address - Wikipedia] : What is RDP and How Does It Work? - CompTIA :CompTIA A+ Certification Exam Core 2 Objectives - CompTIA: Ping (networking utility) - Wikipedia) : IP address - Wikipedia

---

## Question: 277

---

Which of the following filesystems replaced FAT as the preferred filesystem for Microsoft Windows OS?

- A . APFS
- B . FAT32
- C . NTFS
- D . ext4

---

**Answer: C**

---

Explanation:

NTFS stands for New Technology File System and it is the preferred filesystem for Microsoft Windows OS since Windows NT 3.1 in 19931. NTFS replaced FAT (File Allocation Table) as the default filesystem for Windows because it offers many advantages over FAT, such as:

Support for larger volumes and files (up to 16 exabytes)2

Support for file compression, encryption, and permissions2

Support for journaling, which records changes to the filesystem and helps recover from errors2

Support for hard links, symbolic links, and mount points2

Support for long filenames and Unicode characters2

FAT32 is an improved version of FAT that supports larger volumes and files (up to 32 GB and 4 GB respectively) and is compatible with older versions of Windows and other operating systems3. However, FAT32 still has many limitations

and drawbacks compared to NTFS, such as:

No support for file compression, encryption, and permissions3

No support for journaling, which makes it vulnerable to corruption and data loss3

No support for hard links, symbolic links, and mount points3

No support for long filenames and Unicode characters3

APFS (Apple File System) is the default filesystem for macOS, iOS, iPadOS, watchOS, and tvOS since 20174. APFS replaced HFS+ (Hierarchical File System Plus) as the preferred filesystem for Apple devices because it offers many advantages over HFS+, such as:

Support for larger volumes and files (up to 8 zettabytes)4

Support for file cloning, snapshots, and encryption4

Support for space sharing, which allows multiple volumes to share the same storage pool4

Support for fast directory sizing, which improves performance and efficiency4

ext4 (Fourth Extended Filesystem) is the default filesystem for most Linux distributions since 20085. ext4 replaced ext3 as the preferred filesystem for Linux because it offers many advantages over ext3, such as:

Support for larger volumes and files (up to 1 exabyte and 16 terabytes respectively)5

Support for extents, which reduce fragmentation and improve performance5

Support for journal checksumming, which improves reliability and reduces recovery time5

Support for delayed allocation, which improves efficiency and reduces metadata overhead5

1:[NTFS - Wikipedia](#)2: [\[NTFS vs FAT32 vs exFAT: What's the Difference?\]](#)3: [\[FAT32 - Wikipedia\]](#)4: [\[Apple File System - Wikipedia\]](#)5: [\[ext4 - Wikipedia\]](#) : NTFS vs FAT32 vs exFAT: What's the Difference? : FAT32 - Wikipedia : Apple File System - Wikipedia : ext4 - Wikipedia

---

## Question: 278

---

A technician requires graphical remote access to various Windows, Linux, and macOS desktops on the company LAN. The security administrator asks the technician to utilize a single software solution that does not require an external internet connection. Which of the following remote access tools is the technician most likely to install?

- A . VNC
- B . RMM
- C . RDP
- D . SSH

---

**Answer: A**

---

Explanation:

VNC (Virtual Network Computing) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a graphical user interface. VNC does not require an external internet connection, as it works over a local network or a VPN. VNC uses a client-server model, where the server runs on the remote desktop and the client connects to it from another device. VNC can transmit the keyboard and mouse events from the client to the server, and the screen updates from the server to the client, enabling the technician to interact with the remote desktop as if it were local<sup>12</sup>.

VNC is a better option than the other choices because:

RMM (Remote Monitoring and Management) (B) is not a single software solution, but a category of software solutions that enable IT professionals to remotely monitor, manage, and troubleshoot multiple devices and networks. RMM software may include remote access tools, but also other features such as patch management, backup and recovery, security, reporting, and automation. RMM software may require an external internet connection, as it often relies on cloud-based services or web-based consoles<sup>34</sup>.

RDP (Remote Desktop Protocol) is a remote access tool that allows the technician to access and control Windows desktops on the company LAN using a graphical user interface. However, RDP is not compatible with Linux or macOS desktops, unless they have third-party software installed that can emulate or translate the RDP protocol. RDP also has some security and performance issues, such as encryption vulnerabilities, bandwidth consumption, and latency problems<sup>56</sup>.

SSH (Secure Shell) (D) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a command-line interface. SSH does not require an external internet connection, as it works over a local network or a VPN. SSH uses encryption and authentication to secure the communication between the client and the server. However, SSH does not provide a graphical user interface, which may limit the functionality and usability of the remote desktop<sup>7</sup>.

1: What is VNC?- Definition from Techopedia<sup>12</sup> How VNC Works - RealVNC<sup>23</sup> What is Remote Monitoring and Management (RMM)?- Definition from Techopedia<sup>34</sup> What is RMM Software?- NinjaRMM<sup>45</sup> What is Remote Desktop Protocol (RDP)?- Definition from Techopedia<sup>56</sup> Remote Desktop Protocol: What it is and how to secure it - CSO Online<sup>67</sup> What is Secure Shell (SSH)?- Definition from Techopedia<sup>7</sup> How to Use SSH to Access a Remote Server in Linux or Windows - Hostinger Tutorials

---

### Question: 279

---

A user is unable to access a remote server from a corporate desktop computer using the appropriate terminal emulation program. The user contacts the help desk to report the issue. Which of the following clarifying questions would be most effective for the help desk technician to ask the user in

- A . order to understand the issue?
- B . What is the error message?
- C . Does the program work on another computer?
- D . Did the program ever work?
- E . Is anyone else having this issue?

---

Answer: A

---

Explanation:

The most effective clarifying question for the help desk technician to ask the user in order to understand the issue is

A) What is the error message? This question will help the technician to identify the possible cause and solution of the problem, as the error message will provide specific information about the nature and location of the error, such as the server name, the port number, the protocol, the authentication method, or the network status. The error message will also help the technician to troubleshoot the issue by following the suggested steps or searching for the error code online .

This question is more effective than the other choices because:

B) Does the program work on another computer? is not a very helpful question, as it will not reveal the source of the error or how to fix it. The program may work on another computer for various reasons, such as different network settings, firewall rules, permissions, or software versions. However, this question will not tell the technician what is wrong with the user's computer or the remote server, or what needs to be changed or updated to make the program work.

C) Did the program ever work? is not a very relevant question, as it will not address the current issue or how to resolve it. The program may have worked in the past, but it may have stopped working due to changes in the network configuration, the server status, the software updates, or the user credentials. However, this question will not tell the technician what has changed or how to restore the program functionality.

D) Is anyone else having this issue? is not a very useful question, as it will not explain the reason or the solution for the error. The issue may affect only the user, or multiple users, depending on the scope and the impact of the error. However, this question will not tell the technician what is causing the error or how to fix it for the user or the others.

: How to Troubleshoot Terminal Emulation Problems - Techwalla : How to Read and Understand Windows Error Messages - Lifewire : How to Troubleshoot Network Connectivity Problems - How-To Geek : How to Troubleshoot Software Problems - dummies : How to Troubleshoot Common PC Issues For Users - MakeUseOf

---

### **Question: 280**

---

A large organization is researching proprietary software with vendor support for a multiuser environment. Which of the following EULA types should be selected?

- A . Corporate
- B . Perpetual
- C . Open-source
- D . Personal

---

**Answer: A**

---

Explanation:

A corporate EULA is a type of end-user license agreement that is designed for a large organization that needs to use proprietary software with vendor support for a multiuser environment. A corporate EULA typically grants the organization a volume license that allows it to install and use the software on multiple devices or servers, and to distribute the software to its employees or affiliates. A corporate EULA also usually provides the organization with technical support, maintenance, updates, and warranty from the software vendor, as well as some customization

options and discounts. A corporate EULA may also include terms and conditions that specify the rights and obligations of both parties, such as confidentiality, liability, indemnification, termination, and dispute resolution<sup>12</sup>.

A corporate EULA is a better option than the other choices because:

A perpetual EULA (B) is a type of end-user license agreement that grants the user a permanent and irrevocable license to use the software, without any time limit or expiration date. However, a perpetual EULA does not necessarily include vendor support, updates, or warranty, and it may not allow the user to install the software on multiple devices or servers, or to distribute the software to other users. A perpetual EULA may also be more expensive than a corporate EULA, as it requires a one-time payment upfront, rather than a recurring subscription fee<sup>34</sup>.

An open-source EULA is a type of end-user license agreement that grants the user a license to use, modify, and redistribute the software, which is publicly available and free of charge. However, an open-source EULA does not provide any vendor support, maintenance, updates, or warranty, and it may impose some restrictions or obligations on the user, such as disclosing the source code, attributing the original author, or using a compatible license for derivative works. An open-source EULA may not be suitable for a large organization that needs proprietary software with vendor support for a multiuser environment<sup>56</sup>.

A personal EULA (D) is a type of end-user license agreement that grants the user a license to use the software for personal, non-commercial purposes only. A personal EULA may limit the number of devices or servers that the user can install the software on, and prohibit the user from distributing, copying, or reselling the software to other users. A personal EULA may also provide limited or no vendor support, maintenance, updates, or warranty, and it may have a fixed or renewable term. A personal EULA may not meet the needs of a large organization that needs proprietary software with vendor support for a multiuser environment<sup>7</sup>.

1: What is a Corporate License Agreement?- Definition from Techopedia<sup>12</sup> 12: Corporate License Agreement - Template - Word & PDF<sup>23</sup> 23: What is a Perpetual License?- Definition from Techopedia<sup>34</sup> 34: Perpetual vs. Subscription Software Licensing: Which Is Best for You?<sup>45</sup> 45: What is an Open Source License?- Definition from Techopedia<sup>56</sup> 56: Open Source Licenses: Which One Should You Use?<sup>67</sup> 67: What is a Personal License Agreement?- Definition from Techopedia<sup>7</sup> 7: Personal License Agreement - Template - Word & PDF

---

## Question: 281

---

A technician is hardening a company file server and needs to prevent unauthorized LAN devices from accessing stored files. Which of the following should the technician use?

- A . Software firewall
- B . Password complexity
- C . Antivirus application
- D . Anti-malware scans

---

Answer: A

---

Explanation:

A software firewall is a program that monitors and controls the incoming and outgoing network traffic on a computer or a server. A software firewall can help prevent unauthorized LAN devices from accessing stored files on a company file server by applying rules and policies that filter the network packets based on their source, destination, protocol,

port, or content. A software firewall can also block or allow specific applications or services from communicating with the network, and alert the administrator of any suspicious or malicious activity12.

A software firewall is a better option than the other choices because:

Password complexity (B) is a good practice to protect the file server from unauthorized access, but it is not sufficient by itself. Password complexity refers to the use of strong passwords that are hard to guess or crack by attackers, and that are changed frequently and securely. Password complexity can prevent brute force attacks or credential theft, but it cannot stop network attacks that exploit vulnerabilities in the file server software or hardware, or that bypass the authentication process34.

Antivirus application and anti-malware scans (D) are important tools to protect the file server from viruses and malware that can infect, damage, or encrypt the stored files. However, they are not effective in preventing unauthorized LAN devices from accessing the files in the first place. Antivirus and anti-malware tools can only detect and remove known threats, and they may not be able to stop zero-day attacks or advanced persistent threats that can evade or disable them. Moreover, antivirus and anti-malware tools cannot control the network traffic or the file server permissions, and they may not be compatible with all file server platforms or configurations56.

---

1: What is a Firewall and How Does it Work?- Cisco12: How to Harden Your Windows Server - ServerMania23: Password Security: Complexity vs.Length - Norton74: Password Hardening: 5 Ways to Protect Your Passwords - Infosec5: What is Antivirus Software and How Does it Work?- Kaspersky6: What is Anti-Malware? - Malwarebytes

---

### **Question: 282**

---

A branch office suspects a machine contains ransomware. Which of the following mitigation steps should a technician take first?

- A . Disable System Restore.
- B . Remediate the system.
- C . Educate the system user.
- D . Quarantine the system.

---

**Answer: D**

---

Explanation:

The first mitigation step that a technician should take when a machine is suspected to contain ransomware is to quarantine the system. This means isolating the infected machine from the network and other devices, to prevent the ransomware from spreading and encrypting more data.

a.The technician can quarantine the system by disconnecting the network cable, turning off the wireless adapter, or using firewall rules to block the traffic from and to the machine12.

This step is more important than the other options because:

Disabling System Restore (A) is not a priority, as it will not stop the ransomware from running or spreading. System Restore is a feature that allows users to restore their system to a previous state, but it may not work if the ransomware has encrypted or deleted the restore points. Moreover, disabling System Restore may prevent the user from recovering some data or settings in the future13.

Remediating the system (B) is the ultimate goal, but it cannot be done before quarantining the system. Remediating the system means removing the ransomware, restoring the data, and fixing the vulnerabilities that allowed the attack. However, this process requires careful analysis, planning, and execution, and it may not be possible if the ransomware is still active and communicating with the attackers. Therefore, the technician should first isolate the system and then proceed with the remediation steps12.

Educating the system user is a preventive measure, but it is not a mitigation step. Educating the system user means raising awareness and providing training on how to avoid ransomware attacks, such as by recognizing phishing emails, avoiding suspicious links or attachments, and updating and patching the system regularly. However, this step will not help if the system is already infected, and it may not be effective if the user is not willing or able to follow the best practices. Therefore, the technician should focus on resolving the current incident and then educate the user as part of the recovery plan14.

[1: How to Mitigate Ransomware Attacks in 10 Steps - Heimdal Security](#)  
[12: 3 steps to prevent and recover from ransomware | Microsoft Security Blog](#)  
[33: How to use System Restore on Windows 10 | Windows Central](#)  
[54: Ransomware Mitigation | Prevention and Mitigation Strategies - Delinea](#)  
[4](#)

---

### Question: 283

---

A user reports seeing random, seemingly non-malicious advertisement notifications in the Windows 10 Action Center. The notifications indicate the advertisements are coming from a web browser. Which of the following is the best solution for a technician to implement?

- A . Disable the browser from sending notifications to the Action Center.
- B . Run a full antivirus scan on the computer.
- C . Disable all Action Center notifications.
- D . Move specific site notifications from Allowed to Block.

---

**Answer: A**

---

Explanation:

The best solution for a technician to implement is to disable the browser from sending notifications to the Action Center. This will prevent the random advertisement notifications from appearing in the Windows 10 Action Center, which can be annoying and distracting for the user. The technician can follow these steps to disable the browser notifications1:

Open the browser that is sending the notifications, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.

Go to the browser settings or options menu, and look for the privacy and security section.

Find the option to manage site permissions or notifications, and click on it.

You will see a list of sites that are allowed or blocked from sending notifications to the browser and the Action Center. You can either block all sites from sending notifications, or select specific sites that you want to block or allow.

Save the changes and close the browser settings.

This solution is better than the other options because:

Running a full antivirus scan on the computer (B) is not necessary, as the advertisement notifications are not malicious or harmful, and they are not caused by a virus or malware infection. Running a scan will not stop the notifications from appearing, and it will consume system resources and time.

Disabling all Action Center notifications is not advisable, as the Action Center is a useful feature that shows notifications and alerts from various apps and system events, such as email, calendar, security, updates, etc. Disabling all notifications will make the user miss important information and reminders, and reduce the functionality of the Action Center.

Moving specific site notifications from Allowed to Block (D) is not the best solution, as it will only stop the notifications from some sites, but not from others. The user may still receive advertisement notifications from other sites that are not blocked, or from new sites that are added to the Allowed list. This solution will also require the user to manually manage the list of sites, which can be tedious and time-consuming.

[1: How to Disable Annoying Browser Notifications - PCMag](#)

---

### Question: 284

---

A user's Windows computer seems to work well at the beginning of the day. However, its performance degrades throughout the day, and the system freezes when several applications are open. Which of the following should a technician do to resolve the issue? (Select two).

- A . Install the latest GPU drivers.
- B . Reinstall the OS.
- C . Increase the RAM.
- D . Increase the hard drive space.
- E . Uninstall unnecessary software.
- F . Disable scheduled tasks.

---

**Answer: C, E**

---

Explanation:

The most likely causes of the user's Windows computer performance degradation and freezing are insufficient RAM and excessive software running in the background. Therefore, the technician should do the following to resolve the issue:

Increase the RAM. RAM is the memory that the computer uses to store and run applications and processes. If the RAM is not enough to handle the workload, the computer will use the hard drive as a virtual memory, which is much slower and can cause performance issues. Increasing the RAM will allow the computer to run more applications and processes smoothly and avoid freezing. The technician should check the system requirements of the applications that the user needs to run, and install additional RAM modules that are compatible with the motherboard and the existing RAM. The technician should also make sure that the system is managing the page file size automatically, or adjust it manually to optimize the virtual memory usage12.

Uninstall unnecessary software. Software that the user does not need or use can take up valuable disk space and system resources, and can interfere with the performance of other applications. Some software may also run in the background or start automatically when the computer boots up, which can slow down the system and cause freezing. The technician should help the user to identify and uninstall unnecessary software from the control panel

[or the settings app, and disable unnecessary startup programs from the task manager or the system configuration tool.](#) The technician should also check for and remove viruses and malware that may affect the system performance<sup>134</sup>.

[1: Tips to improve PC performance in Windows - Microsoft Support](#)  
[12: How to Upgrade or Install RAM on Your Windows PC - Lifewire](#)  
[53: How to Uninstall Programs on Windows 10 - PCMag](#)  
[64: How to Fix a Windows Computer that Hangs or Freezes - wikiHow](#)

---

### Question: 285

---

Which of the following is the best reason for sandbox testing in change management?

- A . To evaluate the change before deployment
- B . To obtain end-user acceptance
- C . To determine the affected systems
- D . To select a change owner

---

**Answer: A**

---

Explanation:

Sandbox testing is a method of testing changes in a simulated environment that mimics the real one, without affecting the actual production system. Sandbox testing is useful for change management because it allows the testers to evaluate the change before deployment, and ensure that it works as intended, does not cause any errors or conflicts, and meets the requirements and expectations of the stakeholders. Sandbox testing also helps to protect the investment in the existing system, as it reduces the risk of introducing bugs or breaking functionality that could harm the customer experience or the business operations. Sandbox testing also gives the testers more control over the customer experience, as they can experiment with different scenarios and configurations, and optimize the change for the best possible outcome.

[1: Change Management and Sandbox - Quickbase](#)  
[1 2: Embracing change: Build, test, and adapt in a sandbox environment - Zendesk](#)  
[3](#)

---

### Question: 286

---

A Linux technician needs a filesystem type that meets the following requirements:

- . All changes are tracked.
  - . The possibility of file corruption is reduced.
- \* Data recovery is easy.

Which of the following filesystem types best meets these requirements?

- A . ext3
- B . FAT32

- C . exFAT
- D . NTFS

---

**Answer: A**

---

Explanation:

The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:

All changes are tracked. The ext3 file system uses a journaling mechanism that records all changes to the file system metadata in a special log called the journal before applying them to the actual file system. This ensures that the file system can be restored to a consistent state in case of a power failure or system crash12.

The possibility of file corruption is reduced. The journaling feature of ext3 also reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown. The file system can be quickly replayed from the journal and any inconsistencies can be fixed12.

Data recovery is easy. The ext3 file system supports undeletion of files using tools such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them34.

[1: Introduction to Linux File System \[Structure and Types\] - MiniTool](#)[12: 7 Ways to Determine the File System Type in Linux \(Ext2, Ext3 or Ext4\) - Tecmint](#)[13: How to Recover Deleted Files in Linux with ext3grep](#)[4: How to Recover Deleted Files from ext3 Partitions](#)

---

### **Question: 287**

---

A user recently purchased a second monitor and wants to extend the Windows desktop to the new screen. Which of the following Control Panel options should a technician adjust to help the user?

- A . Color Management
- B . System
- C . Troubleshooting
- D . Device Manager
- E . Administrative Tools

---

**Answer: D**

---

---

### **Question: 288**

---

A technician is troubleshooting a Windows 10 PC that is unable to start the GUI. A new SSD and a new copy of Windows were recently installed on the PC. Which of the following is the most appropriate command to use to fix the issue?

- A . msconfig
- B . chkdsk
- C . sfc

- D . diskpart
- E . mstsc

---

Answer: C

---

Explanation:

The sfc command is a tool for scanning and repairing system files that are corrupted or missing on Windows operating systems<sup>1</sup>. System files are essential files that are required for the proper functioning of the operating system, such as the GUI, drivers, services, and applications. If system files are damaged or deleted, the operating system may fail to start or run properly, causing errors, crashes, or blue screens.

The sfc command can be used to fix the issue of the PC that is unable to start the GUI, assuming that the problem is caused by corrupted or missing system files. The sfc command can be run from the command prompt, which can be accessed by booting the PC from the installation media, choosing the repair option, and selecting the command prompt option<sup>3</sup>. The sfc command can be used with different switches, such as /scannow, /verifyonly, /scanfile, or /offbootdir, depending on the situation and the desired action<sup>4</sup>. The most common switch is /scannow, which scans all the system files and repairs any problems that are found<sup>5</sup>. The syntax of the sfc command with the /scannow switch is:

sfc /scannow

The sfc command will then scan and repair the system files, and display the results on the screen. If the sfc command is able to fix the system files, the PC should be able to start the GUI normally after rebooting. If the sfc command is unable to fix the system files, the PC may need further troubleshooting or a clean installation of Windows.

Reference: 1: CompTIA A+ Certification Exam Core 2 Objectives, page 102: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation3:How to use SFC Scannow to repair Windows system files4:SFC Command (System File Checker)5:How to Repair Windows 10 using Command Prompt

---

### Question: 289

---

Which of the following commands can a technician use to get the MAC address of a Linux distribution?

- A . net use
- B . ifconfig
- C . netstat
- D . ping

---

Answer: B

---

Explanation:

The ifconfig command is a tool for configuring network interfaces that any Linux system administrator should know. It is used to bring interfaces up or down, assign and remove addresses and routes, manage ARP cache, and much more<sup>1</sup>. One of the information that ifconfig can display is the MAC address of each network interface, which is a unique identifier of the physical layer of the network device. The MAC address is usually shown as a hexadecimal string separated by colons, such as 00:0c:29:3f:5c:1f. To get the MAC address of a Linux distribution, a technician can

use the ifconfig command without any arguments, which will show the details of all the active network interfaces, or specify the name of a particular interface, such as eth0 or wlan0, to show only the details of that interface.

Reference: 1: Linux Commands - CompTIA A+ 220-1102 - 1.11 - Professor Messer IT Certification Training Courses1

---

### **Question: 290**

---

Which of the following items require special e-waste recycling? (Select two).

- A . Solid-state drive
- B . A/C adapter
- C . Surge protector
- D . Laptop battery
- E . CRT monitor
- F . Power supply

---

**Answer: D, E**

---

Explanation:

Some electronic items require special e-waste recycling because they contain hazardous materials that can harm the environment and human health if disposed of improperly12. Laptop batteries and CRT monitors are examples of such items.

Laptop batteries are usually made of lithium-ion or nickel-metal hydride, which are both toxic and flammable substances34. If laptop batteries are thrown in the trash, they can leak, catch fire, or explode, causing pollution and injuries5. Therefore, laptop batteries should be recycled at authorized collection centers or through manufacturer take-back programs.

CRT monitors are old types of display devices that use cathode ray tubes, which are glass tubes that emit electrons to create images on the screen . CRT monitors contain lead, mercury, cadmium, and phosphor, which are all harmful metals that can contaminate the soil, water, and air if dumped in landfills . Therefore, CRT monitors should be recycled at certified e-waste facilities or through retailer or manufacturer trade-in programs .

Reference: 1: CompTIA A+ Certification Exam Core 2 Objectives, page 132: Environmental Impacts -- CompTIA A+ 220-1102 -- 4.533: The Official CompTIA A+ Core 2 Instructor Guide (Exam 220-1102), page 10-124: CompTIA CertMaster Learn for A+ Core 2 (220-1102) - Student Access Key55: [Why You Should Recycle Your Old Laptop Battery] : [How to Recycle Laptop Batteries] : [Laptop Battery Recycling] : [How to Recycle Laptop Batteries] : The Official CompTIA A+ Core 2 Instructor Guide (Exam 220-1102), page 10-12 : CompTIA CertMaster Learn for A+ Core 2 (220-1102) - Student Access Key : [What is a CRT Monitor?] : [How to Recycle CRT Monitors] : [CRT Monitor Recycling] : [How to Recycle CRT Monitors]

---

### **Question: 291**

---

A developer reports that a workstation's database file extensions have been changed from .db to .enc. The developer is also unable to open the database files manually. Which of the following is the best option for recovering the data?

- A . Accessing a restore point
- B . Rebooting into safe mode
- C . Utilizing the backups
- D . Using an AV to scan the affected files

---

**Answer: C**

---

Explanation:

The scenario described in the question suggests that the workstation has been infected by a ransomware, which is a type of malware that encrypts the files on the target system and demands a ransom for the decryption key<sup>12</sup>.The file extension .enc is commonly used by some ransomware variants to mark the encrypted files<sup>34</sup>. The developer is unable to open the database files manually because they are encrypted and require the decryption key, which is usually held by the attacker.

The best option for recovering the data is to utilize the backups, assuming that the backups are recent, valid, and not affected by the ransomware. Backups are copies of the data that are stored in a separate location or device, and can be used to restore the data in case of a disaster, such as a ransomware attack . By restoring the data from the backups, the developer can avoid paying the ransom and losing the data permanently.

Accessing a restore point is not a good option, because restore points are snapshots of the system settings and configuration, not the data files. Restore points can help to undo some system changes, such as installing a faulty driver or software, but they cannot recover the encrypted data files .

Rebooting into safe mode is also not a good option, because safe mode is a diagnostic mode that allows the system to run with minimal drivers and services, but it does not affect the data files. Safe mode can help to troubleshoot some system issues, such as malware infections, but it cannot decrypt the data files .

Using an AV to scan the affected files is also not a good option, because an AV is a software that can detect and remove some malware, but it cannot decrypt the data files. An AV can help to prevent or remove some ransomware infections, but it cannot recover the encrypted data files .

Reference: 1: CompTIA A+ Certification Exam Core 2 Objectives, page 102: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation  
3:How to remove .enc file virus (Ransomware virus removal guide)  
4:Enc File Extension - What is an .enc file and how do I open it?: CompTIA A+ Certification Exam Core 2 Objectives, page 13 : CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation :What is a restore point?:How to use System Restore on Windows 10: [What is Safe Mode?] : [How to boot into Safe Mode on Windows 10] : CompTIA A+ Certification Exam Core 2 Objectives, page 10 : [Can antivirus software remove ransomware?]

---

## Question: 292

---

A large company is changing its password length requirements. The Chief Information Officer is mandating that passwords now be at least 12 characters long, instead of 10. Which of the following should be used to adjust this setting?

- A . Group Policy
- B . User accounts
- C . Access control lists
- D . Authenticator applications

---

**Answer: A**

---

Explanation:

Group Policy is a feature of Windows that allows administrators to manage and configure settings for computers and users on a network<sup>12</sup>. One of the settings that can be controlled by Group Policy is the password policy, which defines the rules for creating and changing passwords, such as minimum length, complexity, expiration, and history<sup>34</sup>. By using Group Policy, the Chief Information Officer can enforce the new password length requirement for all users and computers in the company's domain, without having to manually adjust each user account or device.

Reference: 1: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-112: CompTIA A+ Certification Exam Core 2 Objectives, page 133: The Official CompTIA A+ Core 2 Instructor Guide (Exam 220-1102), page 10-124: CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives

---

**Question: 293**

---

A technician was assigned a help desk ticket and resolved the issue. Which of the following should the technician update to assist other technicians in resolving similar issues?

- A . End user training
- B . Progress notes
- C . Knowledge base
- D . Acceptable use policy document

---

**Answer: C**

---

Explanation:

A knowledge base is a centralized repository of information that can be used by technicians to find solutions to common problems, best practices, troubleshooting guides, and other useful resources<sup>12</sup>. Updating the knowledge base with the details of the issue and the resolution can help other technicians who encounter similar issues in the future. It can also reduce the number of tickets and improve customer satisfaction<sup>3</sup>.

Reference 1: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-112: CompTIA A+ Certification Exam Core 2 Objectives, page 133: CompTIA A+ Core 2 (220-1102) Certification Study Guide, page 10-12

---

**Question: 294**

---

A corporate smartphone was stored for five months after setup. During this time, the company did not have any system updates. When the phone is turned on, an application runs, but it crashes intermittently. Which of the following should a technician do next?

- A . Restart the phone.
- B . Reimage the OS.

- C . Reinstall the application.
- D . Clear the cache.

---

**Answer: C**

---

Explanation:

Reinstalling the application is the best option to fix the intermittent crashing of the application on the corporate smartphone. Reinstalling the application will ensure that the latest version of the app is installed, which may have bug fixes and compatibility updates that can resolve the crashing issue. Reinstalling the app will also clear any corrupted or outdated data or cache that may cause the app to malfunction.

The other options are not as effective or appropriate as reinstalling the app. Restarting the phone may temporarily fix the issue, but it will not address the root cause of the app crashing, which may be related to the app itself or its data.

a. Reimaging the OS is a drastic and unnecessary measure that will erase all the data and settings on the phone and restore it to its factory state. This will also remove all the other apps and files that may be important for the corporate use of the phone. Clearing the cache may help to free up some space and improve the performance of the app, but it will not update the app or fix any bugs that may cause the app to crash.

[Top 5 Reasons Behind Your App Crash and Solutions To Fix Them1](#)

[How to Stop Apps From Crashing on Android2](#)

[Why are my Android phone apps crashing or closing & how to fix the issue3](#)

---

### **Question: 295**

---

A network technician is deploying a new machine in a small branch office that does not have a DHCP server. The new machine automatically receives the IP address of 169.254.0.2 and is unable to communicate with the rest of the network. Which of the following would restore communication?

- A . Static entry
- B . ARP table
- C . APIPA address
- D . NTP specification

---

**Answer: A**

---

Explanation:

A static entry is the best option to restore communication for the new machine in a small branch office that does not have a DHCP server. A static entry means manually configuring the IP address, subnet mask, default gateway, and DNS server for the network adapter of the machine. A static entry ensures that the machine has a valid and unique IP address that matches the network configuration and can communicate with the rest of the network.

The new machine automatically receives the IP address of 169.254.0.2 because it uses APIPA (Automatic Private IP Addressing), which is a feature that enables computers to self-assign an IP address when a DHCP server is not available. However, APIPA only works for local communication within the same subnet, and does not provide a default gateway or a DNS server. Therefore, the new machine is unable to communicate with the rest of the network, which may be on a different subnet or require a gateway or a DNS server to access.

The other options are not related to restoring communication for the new machine. ARP table is a cache that stores the mapping between IP addresses and MAC addresses for the devices on the network. NTP specification is a protocol that synchronizes the clocks of the devices on the network.

[CompTIA A+ Certification Exam Core 2 Objectives1](#)

[CompTIA A+ Core 2 \(220-1102\) Certification Study Guide2](#)

[What is APIPA \(Automatic Private IP Addressing\)?- Study-CCNA3](#)

[How to Configure a Static IP Address in Windows and OS X4](#)

---

### **Question: 296**

---

An office is experiencing constant connection attempts to the corporate Wi-Fi. Which of the following should be disabled to mitigate connection attempts?

- A . SSID
- B . DHCP
- C . Firewall
- D . SSD

---

**Answer: A**

---

Explanation:

The SSID (Service Set Identifier) is the name of a wireless network that is broadcasted by the router or the Wi-Fi base station. The SSID helps nearby devices to identify and connect to the available networks. However, broadcasting the SSID also exposes the network to potential connection attempts from unauthorized or malicious users. Therefore, disabling the SSID can mitigate connection attempts by making the network invisible or hidden to the devices that are not already connected to it. To connect to a hidden network, the user would need to know the exact SSID and enter it manually.

The other options are not related to mitigating connection attempts to the corporate Wi-Fi. DHCP (Dynamic Host Configuration Protocol) is a protocol that assigns IP addresses to the devices on a network. Firewall is a software or hardware device that filters the incoming and outgoing network traffic based on predefined rules. SSD (Solid State Drive) is a type of storage device that uses flash memory to store data.

- a. Disabling any of these options would not prevent connection attempts to the Wi-Fi network, and may cause other problems or issues for the network functionality and performance.

[What is SSID + how to find \(and change\) it1](#)

## Choosing an SSID2

### SSID Meaning: Finding Your Network's Name3

---

#### **Question: 297**

---

Which of the following would typically require the most computing resources from the host computer?

- A . Chrome OS
- B . Windows
- C . Android
- D . macOS
- E . Linux

---

**Answer: B**

---

Explanation:

Windows is the operating system that typically requires the most computing resources from the host computer, compared to the other options. Computing resources include hardware components such as CPU, RAM, disk space, graphics card, and network adapter. The minimum system requirements for an operating system indicate the minimum amount of computing resources needed to install and run the operating system on a computer. The higher the minimum system requirements, the more computing resources the operating system consumes.

[According to the web search results, the minimum system requirements for Windows 10 and Windows 11 are as follows12:](#)

CPU: 1 GHz or faster with two or more cores (Windows 10); 1 GHz or faster with two or more cores on a compatible 64-bit processor (Windows 11)

RAM: 1 GB for 32-bit or 2 GB for 64-bit (Windows 10); 4 GB (Windows 11)

Disk space: 16 GB for 32-bit or 32 GB for 64-bit (Windows 10); 64 GB (Windows 11)

Graphics card: DirectX 9 or later with WDDM 1.0 driver (Windows 10); DirectX 12 compatible with WDDM 2.0 driver (Windows 11)

Network adapter: Ethernet or Wi-Fi (Windows 10); Ethernet or Wi-Fi that supports 5 GHz (Windows 11)

The minimum system requirements for macOS Ventura are as follows:

CPU: Intel Core i3 or higher, or Apple M1 chip

RAM: 4 GB

Disk space: 35.5 GB

Graphics card: Metal-capable

Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Chrome OS are as follows:

CPU: Intel Celeron or higher

RAM: 2 GB

Disk space: 16 GB

Graphics card: Integrated

Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Android are as follows:

CPU: 1 GHz or higher

RAM: 512 MB

Disk space: 8 GB

Graphics card: OpenGL ES 2.0

Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Linux vary depending on the distribution, but a common example is Ubuntu, which has the following minimum system requirements:

CPU: 2 GHz dual core processor or better

RAM: 4 GB

Disk space: 25 GB

Graphics card: 1024 x 768 screen resolution

Network adapter: Ethernet or Wi-Fi

Based on the comparison of the minimum system requirements, Windows has the highest requirements for CPU, RAM, disk space, and graphics card, while Chrome OS and Android have the lowest requirements. macOS and Linux have moderate requirements, depending on the hardware and software configuration. Therefore, Windows is the operating system that typically requires the most computing resources from the host computer.

[Windows, macOS, Chrome OS, or Linux: Which Operating System Is Right for You?1](#)

[Comparison of operating systems3](#)

[Windows 10 vs 11 Minimum System Requirements: Why Need a New One?2](#)

macOS Monterey - Technical Specifications

Chrome OS - Wikipedia

Android - Wikipedia

Installation/SystemRequirements - Community Help Wiki

---

## **Question: 298**

---

A technician needs to perform after-hours service starting at 10:00 p.m. The technician is currently 20 minutes late. The customer will also be late. Which of the following should the technician do considering proper communication techniques and professionalism?

- A . Do not notify the customer if arriving before the customer.
- B . Dismiss the customer and proceed with the after-hours work.
- C . Contact the customer if the technician is arriving late.
- D . Disclose the experience via social media.

---

## **Answer: C**

---

Explanation:

The best option for the technician to demonstrate proper communication techniques and professionalism is to contact the customer if the technician is arriving late. This shows respect for the customer's time and expectations, and allows the customer to adjust their schedule accordingly. It also helps to maintain a positive relationship and trust between the technician and the customer. The technician should apologize for the delay and provide a realistic estimate of their arrival time. The technician should also thank the customer for their patience and understanding.

The other options are not appropriate or professional. Do not notify the customer if arriving before the customer is not a good practice, as it may cause confusion or frustration for the customer. The customer may have made other plans or arrangements based on the technician's original schedule, and may not be available or prepared for the service. Dismiss the customer and proceed with the after-hours work is rude and disrespectful, as it ignores the customer's needs and preferences. The customer may have questions or concerns about the service, or may want to supervise or verify the work. The technician should always communicate with the customer before, during, and after the service. Disclose the experience via social media is unethical and unprofessional, as it may violate the customer's privacy and the company's policies. The technician should not share any confidential or sensitive information about the customer or the service on social media, or make any negative or inappropriate comments about the customer or the situation.

[CompTIA A+ Certification Exam Core 2 Objectives](#)1

[CompTIA A+ Core 2 \(220-1102\) Certification Study Guide](#)2

[8 Ways You Can Improve Your Communication Skills](#)3

[Professionalism in Communication | How To Do It And How It Pays](#)4

---

## **Question: 299**

---

Which of the following is also known as something you know, something you have, and something you are?

- A . ACL
- B . MFA
- C . SMS
- D . NFC

---

## **Answer: B**

---

Explanation:

MFA stands for Multi-Factor Authentication, which is a method of verifying a user's identity using two or more different factors of authentication. The three factors of authentication are something you know, something you have, and something you are. These factors correspond to different types of information or evidence that only the legitimate user should possess or provide. For example:

Something you know: a password, a PIN, a security question, etc.

Something you have: a smart card, a token, a mobile device, etc.

Something you are: a fingerprint, a face, an iris, etc.

MFA provides a higher level of security than single-factor authentication, which only uses one factor, such as a password. MFA reduces the risk of unauthorized access, identity theft, and data breaches, as an attacker would need to compromise more than one factor to impersonate a user. MFA is commonly used for online banking, email accounts, cloud services, and other sensitive applications

---

## **Question: 300**

---

A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

- A . Run an antivirus and enable encryption.
- B . Restore the defaults and reimage the corporate OS.
- C . Back up the files and do a system restore.
- D . Undo the jailbreak and enable an antivirus.

---

## **Answer: B**

---

Explanation:

The best course of action for the technician is to restore the defaults and reimage the corporate OS on the device. This will remove the jailbreak and any unauthorized or malicious apps that may have been installed on the device, as well as restore the security features and policies that the company has set for its devices. This will also ensure that the device can receive the latest updates and patches from the manufacturer and the company, and prevent any data leakage or compromise from the device.

Jailbreaking is a process of bypassing the built-in security features of a device to install software other than what the manufacturer has made available for that device. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features. However, jailbreaking also exposes the device to various risks, such as:

The loss of warranty from the device manufacturers.

[Inability to update software until a jailbroken version becomes available2.](#)

[Increased security vulnerabilities32.](#)

[Decreased battery life2.](#)

[Increased volatility of the device2.](#)

Some of the signs of a jailbroken device are:

[A high number of ads, which may indicate the presence of adware or spyware on the device3.](#)

[Receiving data-usage limit notifications, which may indicate the device is sending or receiving data in the background without the user's knowledge or consent3.](#)

[Experiencing slow response, which may indicate the device is running unauthorized or malicious apps that consume resources or interfere with the normal functioning of the device3.](#)

[Finding apps or icons that the user did not install or recognize, such as Cydia, which is a storefront for jailbroken iOS devices1.](#)

The other options are not sufficient or appropriate for dealing with a jailbroken device. Running an antivirus and enabling encryption may not detect or remove all the threats or vulnerabilities that the jailbreak has introduced, and may not restore the device to its original state or functionality. Backing up the files and doing a system restore may not erase the jailbreak or the unauthorized apps, and may also backup the infected or compromised files. Undoing the jailbreak and enabling an antivirus may not be possible or effective, as the jailbreak may prevent the device from updating or installing security software, and may also leave traces of the jailbreak or the unauthorized apps on the device.

[CompTIA A+ Certification Exam Core 2 Objectives4](#)

[CompTIA A+ Core 2 \(220-1102\) Certification Study Guide5](#)

[What is Jailbreaking & Is it safe?- Kaspersky1](#)

[Is Jailbreaking Safe?The ethics, risks and rewards involved - Comparitech3](#)

[Jailbreaking : Security risks and moving.past them2](#)

---

### **Question: 301**

---

A customer calls desktop support and begins yelling at a technician. The customer claims to have submitted a support ticket two hours ago and complains that the issue still has not been resolved. Which of the following describes how the technician should respond?

- A . Place the customer on hold until the customer calms down.
- B . Disconnect the call to avoid a confrontation.
- C . Wait until the customer is done speaking and offer assistance.
- D . Escalate the issue to a supervisor.

Explanation:

The best way to deal with an angry customer who is yelling at a technician is to wait until the customer is done speaking and offer assistance. This shows respect, empathy, and professionalism, and allows the technician to understand the customer's problem and find a solution. According to the CompTIA A+ Core 2 (220-1102) Certification Study Guide1, some of the steps to handle angry customers are:

Stay calm and do not take it personally.

Listen actively and acknowledge the customer's feelings.

Apologize sincerely and offer to help.

Restate the customer's issue and ask for clarification if needed.

Explain the possible causes and solutions for the problem.

Provide clear and realistic expectations for the resolution.

Follow up with the customer until the issue is resolved.

The other options are not appropriate ways to deal with angry customers, as they may worsen the situation or damage the customer relationship. Placing the customer on hold may make them feel ignored or dismissed. Disconnecting the call may make them feel disrespected or abandoned. Escalating the issue to a supervisor may make them feel frustrated or powerless, unless the technician cannot resolve the issue or the customer requests to speak to a supervisor.

[CompTIA A+ Certification Exam Core 2 Objectives2](#)

[CompTIA A+ Core 2 \(220-1102\) Certification Study Guide1](#)

[How To Deal with Angry Customers \(With Examples and Tips\)3](#)

[17 ways to deal with angry customers: Templates and examples4](#)

[Six Ways to Handle Angry Customers5](#)

---

### **Question: 302**

---

When a user is in the office, the user's mobile phone loads applications and web browses very slowly on a cellular connection. Which of the following is the best way to fix this issue?

- A . Connect to the company's Wi-Fi network.
- B . Change the settings on the phone to connect to a different cellular tower.
- C . Install a cellular repeater at the office for this user.
- D . Update all applications on the phone.

---

**Answer: A**

---

Explanation:

The best way to fix the issue of slow cellular connection in the office is to connect to the company's Wi-Fi network. This will allow the user's mobile phone to access the internet through a faster and more reliable wireless network, instead of relying on the cellular network. Connecting to the Wi-Fi network will also save the user's data usage and battery life.

Some of the factors that can affect the cellular connection speed are the distance from the cell tower, the obstructions between the phone and the tower, the network congestion, the network technology, and the features of the phone<sup>12</sup>. In the office, the user may experience a weak or unstable cellular signal due to the building structure, the location, or the interference from other devices. Therefore, switching to the Wi-Fi network can improve the performance of the phone's applications and web browsing.

[CompTIA A+ Certification Exam Core 2 Objectives](#)<sup>3</sup>

[CompTIA A+ Core 2 \(220-1102\) Certification Study Guide](#)<sup>4</sup>

[Factors affecting the speed and quality of internet connection](#)<sup>1</sup>

[Why Is Your Mobile Data So Slow? How to Speed It Up in 10 Steps](#)<sup>2</sup>

---

**Question: 303**

---

A hotel's Wi-Fi was used to steal information on a corporate laptop. A technician notes the following security log:

SRC: 192.168.1.1/secrets.zip Protocol SMB >> DST: 192.168.1.50/capture

The technician analyses the following Windows firewall information:

Port	Status	Direction
1	Open	In/Out
445	Open	In/Out
25	Open	Out
110	Open	In/Out
53	Open	In/Out

Which of the following protocols most likely allowed the data theft to occur?

- A . 1
- B . 53
- C . 110
- D . 445

---

**Answer: D**

---

## Explanation:

The protocol that most likely allowed the data theft to occur is SMB over TCP port 445. SMB is a network file sharing protocol that enables access to files, printers, and other resources on a network. Port 445 is used by SMB to communicate directly over TCP without the need for NetBIOS, which is an older and less secure protocol. The security log shows that the source IP address 192.168.1.1 sent a file named secrets.zip using SMB protocol to the destination IP address 192.168.1.50, which captured the file. The Windows firewall information shows that port 445 is enabled for inbound and outbound traffic, which means that it is not blocked by the firewall. Therefore, port 445 is the most likely port that was exploited by the attacker to steal the data from the corporate laptop.

[SMB port number: Ports 445, 139, 138, and 137 explained1](#)

[What is an SMB Port + Ports 445 and 139 Explained2](#)

[CompTIA A+ Certification Exam Core 2 Objectives3](#)

---

## Question: 304

---

### SIMULATION

As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer. Corporate policy requires he following:

- . All phishing attempts must be reported.
- . Future spam emails to users must be prevented.

### INSTRUCTIONS

Review each email and perform the

following within the email:

- . Classify the emails
- . Identify suspicious items, if applicable, in each email
- . Select the appropriate resolution



# Inbox

## Account Locked

Dear User, We have detected unusual activity com...

## Share Your Feedback

It only takes 4 minutes of your time! In partners...

## Employee Orientation

Dear Joe, Welcome to CompTIA! We are excited...

## Security Update

We need to install an urgent patch to your Windows...

## Interview

Good afternoon Joe, I just wanted to thank you for



## No Mail Selected

Select an email to view its contents

## Email Class

### Classification

### Resolution

- Report email
- Perform no action
- Unsubscribe
- Open attachment

A . Report email to Information Security. The user should not click on the link, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report the phishing attempt. The user should also delete the email from their inbox and trash folder.

The suspicious items to select are:

- b) From address
- d) Hyperlinks

These items indicate that the email is not from a legitimate source and that the link is potentially malicious. The

other items are not suspicious in this case, as the to address is the user's own email and there are no attachments.

## Inbox

### Account Locked

Dear User, We have detected unusual activity com...

### Share Your Feedback

It only takes 4 minutes of your time! In partners...

### Employee Orientation

Dear Joe, Welcome to CompTIA!  
We are excited...

### Security Update

We need to install an urgent patch to your Windows...

### Interview

Good afternoon Joe, I just wanted to thank you for

**From:** ithelpdesk@comptia.co

**Subject:** Account Locked

**To:** joe@comptia.org

Dear User,

We have detected unusual activity coming from your corporate account joe@comptia.org.  
To protect your account, please click [HERE](#) to change your password.

Regards,

CompTIA IT Help Desk

### Email Classification

#### Classification

Phishing

#### Suspicious items

To address

From address

Attachments

Hyperlinks

#### Resolution

Report email to Info

Perform no addition

Unsubscribe

Open attachment

### Classification: b) Spam

This email is a spam email, as it is an unsolicited and unwanted message that tries to persuade the user to participate in a survey and claim a reward. Some suspicious items in this email are:

The email offers a free wireless headphone as an incentive, which is too good to be true.

The email does not provide any details about the survey company, such as its name, address, or contact information.

The email contains an external survey link, which may lead to a malicious or fraudulent website.

The email does not have an unsubscribe option, which is required by law for commercial emails.

The appropriate resolution for this email is C. Unsubscribe. The user should look for an unsubscribe link or button at the bottom of the email and follow the instructions to opt out of receiving future emails from the sender. The user should also mark the email as spam or junk in their email client, which will help filter out similar emails in the future.

The user should not click on the survey link, reply to the email, or provide any personal or financial information.

**From:** survey@researchco.net  
**Subject:** Share Your Feedback And Get Free Wireless Headphones!  
**To:** joe@comptia.org  
**Signed By:** survey@researchco.net



**External Email**

It only takes 4 minutes of your time!

In partnership with Research & Co. we are conducting a survey regarding your cellular service. As an expert in your field, we'd love to get your feedback!

This quick survey will only take a few minutes of your time, and as a token of our appreciation for sharing your insight, you will receive a pair of wireless headphones.

[Take the Survey here!](#)

[Manage Email Preferences](#)

**Email Classification Menu**

**Classification**

Spam

**Resolution**

Report email to Information Security  
 Perform no additional actions  
 Unsubscribe  
 Open attachment

Classification: c) Legitimate

This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, the attachment, and the email body are all consistent and relevant. The appropriate resolution for this email is B. Perform no additional actions. The user can open the attachment and review the orientation material as instructed. The user does not need to report, unsubscribe, or delete this email.

**From:** Human Resources <hr@comptia.org>  
**Subject:** Employee Orientation  
**To:** joe@comptia.org  
 Employee\_Reference\_Guide.PDF

Dear Joe,

Welcome to CompTIA!

We are excited that you are here, and we know you will be a valuable asset to the company.

Please review the attached orientation material to get started with the onboarding experience.

Regards,  
CompTIA Human Resources

**Email Classification Menu**

**Classification**

Legitimate

**Resolution**

Report email to Information Security  
 Perform no additional actions  
 Unsubscribe  
 Open attachment

Classification: a) Phishing

This email is a phishing attempt, as it tries to deceive the user into downloading and running a malicious attachment

that could compromise their system or data. Some suspicious items in this email are:

The email has a generic greeting and does not address the user by name or username.

The email has an urgent tone and claims that a security patch needs to be installed immediately.

The email has an attachment named "patch1.exe", which is an executable file that could contain malware or ransomware.

The email does not match the official format or domain of CompTIA Information Security.

The appropriate resolution for this email is A. Report email to Information Security. The user should not open the attachment, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report the phishing attempt. The user should also delete the email from their inbox and trash folder.

**From:** CompTIA Information Security <infosec@comptia.org>  
**Subject:** Security Update  
**To:** joe@comptia.org  
🔗 patch1.exe

We need to install an urgent patch to your Windows Operating System. Please download and run the included attachment to install the security patch as soon as possible!

Regards,  
CompTIA Information Security  
infosec@comptia.org

### Email Classification Menu

#### Classification

Phishing

#### Suspicious items

- To address
- From address
- Attachments
- Hyperlinks

#### Resolution

- Report email to Information Security
- Perform no additional actions
- Unsubscribe
- Open attachment

# Inbox

## Account Locked

Dear User, We have detected unusual activity com...

## Share Your Feedback

It only takes 4 minutes of your time! In partners...

## Employee Orientation

Dear Joe, Welcome to CompTIA!  
We are excited...

## Security Update

We need to install an urgent patch to your Windows...

## Interview

Good afternoon Joe, I just wanted to thank you for

**From:** Human Resources <hr@comptia.org>  
**Subject:** Employee Orientation  
**To:** joe@comptia.org  
 Employee\_Reference\_Guide.PDF

## Email Classification

### Classification

Legitimate

### Resolution

Report email to Info

Perform no additional actions

Unsubscribe

Open attachment

Classification: c) Legitimate

This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, and the email body are all consistent and relevant. The appropriate resolution for this email is B. Perform no additional actions. The user can reply to the email and thank the sender for the interview opportunity. The user does not need to report, unsubscribe, or delete this email.

**From:** Alex <alex@gmail.com>  
**Subject:** Interview  
**To:** joe@comptia.org

Good afternoon Joe,

I just wanted to thank you for your time during my interview last week. It was exciting to hear about the position and possible opportunity at CompTIA. Please don't hesitate to reach out to me with any questions or concerns you may have about me or my qualifications. Regardless of the outcome, it was a pleasure speaking with you, and I hope to have the opportunity to work with you in the future.

Regards,  
Alex

## Email Classification Menu

### Classification

Legitimate

### Resolution

Report email to Information Security

Perform no additional actions

Unsubscribe

Open attachment

A . See the Full solution in Explanation below

---

**Answer: A, A**

---

Explanation:

Classification: a) Phishing

This email is a phishing attempt, as it tries to trick the user into clicking on a malicious link that could compromise their account or personal information. Some suspicious items in this email are:

The email has a generic greeting and does not address the user by name.

The email has spelling errors, such as "unusal" and "Locaked".

The email uses a sense of urgency and fear to pressure the user into clicking on the link.

The email does not match the official format or domain of the IT Help Desk at CompTIA.

The email has two black bat icons, which are not related to CompTIA or IT support.

The appropriate resolution for this email is

---

### **Question: 305**

---

A technician is building a new desktop machine for a user who will be using the workstation to render 3-D promotional movies. Which of the following is the most important component?

- A . Dedicated GPU
- B . DDR5 SODIMM
- C . NVMe disk
- D . 64-bit CPU

---

**Answer: A**

---

Explanation:

A dedicated GPU (graphics processing unit) is the most important component for rendering 3-D promotional movies, as it can handle the complex calculations and graphics operations required for creating realistic and high-quality images. A dedicated GPU has its own memory and processor, which are optimized for graphics tasks. A dedicated GPU can also support multiple monitors, high resolutions, and advanced features such as ray tracing12.

---

### **Question: 306**

---

A user requested that the file permissions on a Linux device be changed to only allow access to a certain group of users. Which of the following commands should be used to complete the user's request?

- A . cat
- B . chmod
- C . pwd
- D . cacls

---

**Answer: B**

---

Explanation:

The chmod command is used to change the permissions of files and directories in Linux. It can grant or revoke read, write, and execute permissions for the owner, the group, and others. To change the file permissions to only allow access to a certain group of users, the chmod command can use either the symbolic or the numeric mode. For example, to give read and write permissions to the group and no permissions to others, the command can be:

chmod g+rwx,o-rwx filename

or

chmod 660 filename

---

### **Question: 307**

---

An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

- A . Risk analysis
- B . Sandbox testing
- C . End user acceptance
- D . Lessons learned

---

**Answer: A**

---

Explanation:

Risk analysis is the process of identifying and evaluating the potential threats and impacts of a change on the system, network, or service. It is an essential step before approving a change request, as it helps to determine the level of risk, the mitigation strategies, and the contingency plans. Risk analysis also helps to prioritize the change requests based on their urgency and importance<sup>12</sup>.

---

### **Question: 308**

---

A user wants to acquire antivirus software for a SOHO PC. A technician recommends a licensed software product, but the user does not want to pay for a license. Which of the following license types should the technician recommend?

- A . Corporate

- B . Open-source
- C . Personal
- D . Enterprise

---

**Answer: B**

---

Explanation:

Open-source software is software that has its source code available for anyone to inspect, modify, and distribute. Open-source software is usually free of charge and does not require a license to use. Some examples of open-source antivirus software are ClamAV, Comodo, and Immunet12. The other license types are either not free or not suitable for a SOHO PC. Corporate and enterprise licenses are designed for large-scale organizations and networks, and they usually require a subscription fee. Personal licenses are for individual users and may have limited features or support.

---

### **Question: 309**

---

Which of the following environmental factors are most important to consider when planning the configuration of a data center? (Select two).

- A . Temperature levels
- B . Location of the servers
- C . Humidity levels
- D . Noise levels
- E . Lighting levels
- F . Cable management

---

**Answer: A, C**

---

Explanation:

Temperature and humidity levels are the most important environmental factors to consider when planning the configuration of a data center, as they directly affect the performance, reliability, and energy efficiency of the IT equipment. Excessive heat or moisture can cause overheating, corrosion, condensation, or static electricity, which can damage the hardware and lead to data loss or service disruption. Therefore, data centers need to monitor and control the temperature and humidity levels within the recommended ranges by using various cooling systems, airflow management, and sensors12.

---

### **Question: 310**

---

When visiting a particular website, a user receives a message stating, 'Your connection is not private.' Which of the following describes this issue?

- A . Certificate warning
- B . Malware
- C . JavaScript error

D . Missing OS update

---

**Answer: A**

---

Explanation:

A certificate warning is a message that appears when a web browser cannot verify the identity or security of a website. It usually means that there is a problem with the website's SSL certificate, such as expiration, invalidity, or mismatch. A certificate warning can indicate that the website is unsafe or compromised, and that the user's connection is not private123.

---

### **Question: 311**

---

The calendar application on an employee's smartphone is experiencing frequent crashes, and the smartphone has become unresponsive. Which of the following should a technician do first to resolve the issue?

- A . Reinstall the application on the smartphone.
- B . Update the smartphone's OS.
- C . Reset the smartphone to factory settings.
- D . Reboot the smartphone.

---

**Answer: D**

---

Explanation:

Rebooting the smartphone is the first and simplest step to resolve the issue of frequent crashes and unresponsiveness. Rebooting clears the memory, closes the background apps, and refreshes the system. It can also fix minor glitches and bugs that may cause the calendar app or the smartphone to malfunction12. The other options are either too drastic or unnecessary. Reinstalling the application may not solve the problem if the issue is with the smartphone itself. Updating the smartphone's OS may not be possible or helpful if the device is unresponsive or incompatible. Resetting the smartphone to factory settings will erase all the data and settings on the device, which should be the last resort.

---

### **Question: 312**

---

An organization is creating guidelines for the incorporation of generative AI solutions. In which of the following would these guidelines be published?

- A . Standard operating procedure
- B . Acceptable use policy
- C . Security protocols
- D . Data flow diagram

---

**Answer: B**

---

Explanation:

An acceptable use policy (AUP) is a document that defines the rules and expectations for the users of a system, network, or service. It typically covers topics such as the purpose, scope, responsibilities, and restrictions of using the system, network, or service<sup>1</sup>. An AUP is a suitable place to publish the guidelines for the incorporation of generative AI solutions, as it can inform the users of the benefits, risks, and ethical implications of using such tools. It can also specify the conditions and limitations for using generative AI solutions, such as the types of data, content, and applications that are allowed or prohibited, the security and privacy requirements, the legal and regulatory compliance, and the accountability and reporting mechanisms<sup>23</sup>.

---

### Question: 313

---

Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed first to prevent further damage to the host and other systems?

- A . Turn off the machine.
- B . Run a full antivirus scan.
- C . Remove the LAN card.
- D . Install a different endpoint solution.

---

Answer: A

---

Explanation:

Turning off the machine is the first and most urgent step to prevent further damage to the host and other systems. Ransomware can encrypt files, steal data, and spread to other devices on the network if the infected machine remains online. Turning off the machine will stop the ransomware process and isolate the machine from the network<sup>12</sup>. The other options are either ineffective or risky. Running a full antivirus scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Removing the LAN card may disconnect the machine from the network, but it will not stop the ransomware from encrypting or deleting files on the local drive. Installing a different endpoint solution may not be possible or helpful if the ransomware has already compromised the system or blocked the installation.

---

### Question: 314

---

A technician downloaded a software program to a network share. When the technician attempts to copy the program to the Windows tablet for installation, the technician receives an error. Which of the following is the best procedure for the technician to use to complete the assignment?

- A . Copy the program file to a USB drive and install.
- B . Burn the program file to a CD and install.
- C . Format the HDD and then do the installation.
- D . Replace the HDD and then do the installation.

Explanation:

Copying the program file to a USB drive and installing it from there is the simplest and most reliable way to transfer the software from the network share to the Windows tablet. The other options are either unnecessary, risky, or impractical. Burning the program file to a CD requires a CD burner and a CD reader, which may not be available on the tablet. Formatting or replacing the HDD will erase all the data and settings on the tablet, which is not advisable unless there is a backup or a serious problem. Moreover, formatting or replacing the HDD will not solve the issue of copying the program file from the network share.

---

**Question: 315**

---

A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

- A . Run an antivirus and enable encryption.
- B . Restore the defaults and reimage the corporate OS.
- C . Back up the files and do a system restore.
- D . Undo the jailbreak and enable an antivirus.

Explanation:

Jailbreaking a device exposes it to various security risks, such as malware, data theft, network attacks, and service disruption<sup>1234</sup>. Running an antivirus and enabling encryption may not be enough to remove the threats and restore the device's functionality. Undoing the jailbreak may not be possible or effective, depending on the method used. Backing up the files and doing a system restore may preserve the jailbreak and the associated problems. The best option is to erase the device and reinstall the original operating system that is compatible with the corporate policies and standards. This will ensure that the device is clean, secure, and compliant<sup>25</sup>.

---

**Question: 316**

---

An organization is updating the monitors on kiosk machines. While performing the upgrade, the organization would like to remove physical input devices. Which of the following utilities in the Control Panel can be used to turn on the on-screen keyboard to replace the physical input devices?

- A . Devices and Printers
- B . Ease of Access
- C . Programs and Features
- D . Device Manager

---

**Answer: B**

---

Explanation:

Ease of Access is a utility in the Control Panel that allows users to adjust various accessibility settings on Windows, such as the on-screen keyboard, magnifier, narrator, high contrast, etc. The on-screen keyboard can be turned on by going to Ease of Access > Keyboard and toggling the switch to On. Alternatively, the on-screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box. 3.

---

### **Question: 317**

---

Which of the following file types allows a user to easily uninstall software from macOS by simply placing it in the trash bin?

- A .exe
- B .dmg
- C .app
- D .rpm
- E .pkg

---

**Answer: C**

---

Explanation:

.app files are application bundles that contain all the necessary files and resources for a Mac app. They can be easily deleted by dragging them to the Trash or using Launchpad. 12. Other file types, such as .exe, .dmg, .rpm, and .pkg, are either not compatible with macOS or require additional steps to uninstall. 34.

---

### **Question: 318**

---

Which of the following statements describes the purpose of scripting languages?

- A . To access the hardware of the computer it is running on
- B . To automate tasks and reduce the amount of manual labor
- C . To abstract the complexity of the computer system
- D . To compile the program into an executable file

---

**Answer: B**

---

Explanation:

Scripting languages are used to write small to medium-sized programs that perform specific tasks. Some common uses of scripting languages are: automating repetitive processes, web development, system administration, data

[processing, multimedia and games, report generation, document and text processing, writing.plugins and extensions for existing programs and applications1.](#)

---

### Question: 319

---

Maintaining the chain of custody is an important part of the incident response process. Which of the following reasons explains why this is important?

- A . To maintain an information security policy
- B . To properly identify the issue
- C . To control evidence and maintain integrity
- D . To gather as much information as possible

---

**Answer: C**

---

Explanation:

Maintaining the chain of custody is important to control evidence and maintain integrity. The chain of custody is a process that documents who handled, accessed, or modified a piece of evidence, when, where, how, and why. The chain of custody ensures that the evidence is preserved, protected, and authenticated throughout the incident response process. Maintaining the chain of custody can help prevent tampering, alteration, or loss of evidence, as well as establish its reliability and validity in legal proceedings. Maintaining an information security policy, properly identifying the issue, and gathering as much information as possible are not reasons why maintaining the chain of custody is important. Maintaining an information security policy is a general practice that defines the rules and guidelines for securing an organization's information assets and resources. Properly identifying the issue is a step in the incident response process that involves analyzing and classifying the incident based on its severity, impact, and scope. Gathering as much information as possible is a step in the incident response process that involves collecting and documenting relevant data and evidence from various sources, such as logs, alerts, or witnesses. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 26](#)

---

### Question: 320

---

A technician successfully removed malicious software from an infected computer after running updates and scheduled scans to mitigate future risks. Which of the following should the technician do next?

- A . Educate the end user on best practices for security.
- B . Quarantine the host in the antivirus system.
- C . Investigate how the system was infected with malware.
- D . Create a system restore point.

---

**Answer: A**

---

Explanation:

Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end user on best practices for security can help the end user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections. Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware. Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken. Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system's configuration and settings at a certain point in time, which can be used to restore the system in case of failure or corruption. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Cert Guide, page 458](#)

---

### Question: 321

---

A systems administrator received a request to limit the amount of cellular data a user's Windows 10 tablet can utilize when traveling. Which of the following can the administrator do to best solve the user's issue?

- A . Turn on airplane mode.
- B . Set the connection to be metered.
- C . Configure the device to use a static IP address.
- D . Enable the Windows Defender Firewall.

---

**Answer: B**

---

Explanation:

Setting the connection to be metered is the best solution for limiting the amount of cellular data a user's Windows 10 tablet can utilize when traveling. A metered connection is a network connection that has a data limit or charges fees based on the amount of data used. Windows 10 allows users to set any network connection as metered, which reduces the amount of data that Windows and some apps use in the background. For example, setting a connection as metered will prevent Windows from downloading updates automatically, stop some apps from syncing data online, and disable some live tiles on the Start menu. Setting a connection as metered can help users save cellular data and avoid extra charges when traveling. Turning on airplane mode, configuring the device to use a static IP address, and enabling the Windows Defender Firewall are not effective solutions for limiting the amount of cellular data a user's Windows 10 tablet can utilize when traveling. Turning on airplane mode will disable all wireless connections on the device, including Wi-Fi, Bluetooth, and cellular data. This will prevent the user from accessing any online services or applications on the tablet. Configuring the device to use a static IP address will assign a fixed IP

address to the device instead of obtaining one dynamically from a DHCP server. This will not affect the amount of cellular data the device uses, and it may cause IP conflicts or connectivity issues on some networks. Enabling the Windows Defender Firewall will block or allow incoming and outgoing network traffic based on predefined or custom rules. This will not reduce the amount of cellular data the device uses, and it may interfere with some apps or services that require network access.Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 19](#)

[CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 108](#)

---

### Question: 322

---

Which of the following file types would be used in the Windows Startup folder to automate copying a personal storage table (.pst file) to a network drive at log-in?

- A .bat
- B .dll
- C .ps1
- D .txt

---

**Answer: A**

---

Explanation:

The .bat file type would be used in the Windows Startup folder to automate copying a personal storage table (.pst) file to a network drive at log-in. A .bat file is a batch file that contains a series of commands that can be executed by the command interpreter. A .bat file can be used to perform various tasks, such as copying, moving, deleting, or renaming files or directories. A .bat file can be placed in the Windows Startup folder to run automatically when a user logs in to the system. A .bat file can use the copy command to copy a .pst file from a local drive to a network drive. A .pst file is a personal storage table file that contains email messages, contacts, calendars, and other data from Microsoft Outlook. A .pst file can be backed up to a network drive for security or recovery purposes. The .dll, .ps1, and .txt file types are not used in the Windows Startup folder to automate copying a .pst file to a network drive at log-in. A .dll file is a dynamic link library file that contains code or data that can be shared by multiple programs. A .dll file cannot be executed directly by the user or the system. A .ps1 file is a PowerShell script file that contains commands or expressions that can be executed by the PowerShell interpreter. A .ps1 file can also perform various tasks, such as copying files or directories, but it requires PowerShell to be installed and configured on the system. A .txt file is a plain text file that contains unformatted text that can be read by any text editor or word processor. A .txt file cannot contain commands or expressions that can be executed by the system.Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 18](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Cert Guide, page 459](#)

---

### Question: 323

---

Which of the following is command options is used to display hidden files and directories?

- A . -a
- B . -s
- C . -lh
- D . -t

---

**Answer: A**

---

Explanation:

The -a option is used to display hidden files and directories in a command-line interface. Hidden files and directories are those that start with a dot (.) and are normally not shown by default. The -a option stands for "all" and shows all files and directories, including the hidden ones. The -a option can be used with commands such as ls, dir, or find to list or search for hidden files and directories. The -s, -lh, and -t options are not used to display hidden files and directories. The -s option stands for "size" and shows the size of files or directories in bytes. The -lh option stands for "long human-readable" and shows the size of files or directories in a more readable format, such as KB, MB, or GB. The -t option stands for "time" and sorts the files or directories by modification time. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 17](#)

[CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 107](#)

---

### Question: 324

---

Which of the following is used to ensure users have the appropriate level of access to perform their job functions?

- A . Access control list
- B . Multifactor authentication
- C . Least privilege
- D . Mobile device management

---

**Answer: C**

---

Explanation:

Least privilege is the principle that is used to ensure users have the appropriate level of access to perform their job functions. Least privilege means granting users only the minimum amount of access rights and permissions they need to perform their tasks, and nothing more. Least privilege reduces the risk of unauthorized access, data leakage, malware infection, or accidental damage by limiting what users can do on the system or network. Access control list, multifactor authentication, and mobile device management are not principles, but rather mechanisms or methods that can implement least privilege. Access control list is a list that specifies the users or groups that are allowed or denied access to a resource, such as a file, folder, or printer. Multifactor authentication is a method that requires users to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Mobile device management is a tool that allows managing and securing mobile devices, such as smartphones or tablets, that are used by employees to access corporate data or applications. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25](#)

[CompTIA Security+ SY0-601 Certification Study Guide], page 1003

---

## **Question: 325**

---

A company is recycling old hard drives and wants to quickly re-provision the drives for reuse. Which of the following data destruction methods should the company use?

- A . Degaussing
- B . Standard formatting
- C . Low-level wiping
- D . Deleting

---

**Answer: C**

---

Explanation:

Low-level wiping is the best data destruction method for recycling old hard drives for reuse. Low-level wiping is a process that overwrites every bit of data on a hard drive with zeros or random patterns, making it impossible to recover any data from the drive. Low-level wiping also restores the drive to its factory state, removing any bad sectors or errors that may have accumulated over time. Low-level wiping can be done using specialized software tools or hardware devices that connect to the drive. Degaussing, standard formatting, and deleting are not suitable data destruction methods for recycling old hard drives for reuse. Degaussing is a process that exposes a hard drive to a strong magnetic field, destroying both the data and the drive itself. Degaussing renders the drive unusable for reuse. Standard formatting is a process that erases the data on a hard drive by removing the file system structure, but it does not overwrite the data itself. Standard formatting leaves some data recoverable using forensic tools or software utilities. Deleting is a process that removes the data from a hard drive by marking it as free space, but it does not erase or overwrite the data itself. Deleting leaves most data recoverable using undelete tools or software utilities.

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15](#)

[CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105](#)

---

## **Question: 326**

---

A technician receives an invalid certificate error when visiting a website. Other workstations on the same local network are unable to replicate this issue. Which of the following is most likely causing the issue?

- A . Date and time
- B . User access control
- C . UEFI boot mode
- D . Log-on times

---

**Answer: A**

---

Explanation:

Date and time is the most likely cause of the issue. The date and time settings on a workstation affect the validity of the certificates used by websites to establish secure connections. If the date and time are incorrect, the workstation may not recognize the certificate as valid and display an invalid certificate error. Other workstations on the same local network may not have this issue if their date and time are correct. User access control, UEFI boot mode, and log-on times are not likely causes of the issue. User access control is a feature that prevents unauthorized changes to the system by prompting for confirmation or credentials. UEFI boot mode is a firmware interface that controls the boot process of the workstation. Log-on times are settings that restrict when a user can log in to the workstation. None of these factors affect the validity of the certificates used by websites. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Cert Guide, page 456](#)

---

### Question: 327

---

A technician needs administrator access on a Windows workstation to facilitate system changes without elevating permissions. Which of the following would best accomplish this task?

- A . Group Policy Editor
- B . Local Users and Groups
- C . Device Manager
- D . System Configuration

---

**Answer: B**

---

Explanation:

Local Users and Groups is the best option to accomplish this task. Local Users and Groups is a tool that allows managing the local user accounts and groups on a Windows workstation. The technician can use this tool to create a new user account with administrator privileges or add an existing user account to the Administrators group. This way, the technician can log in with the administrator account and make system changes without elevating permissions. Group Policy Editor, Device Manager, and System Configuration are not correct answers for this question. Group Policy Editor is a tool that allows configuring policies and settings for users and computers in a domain environment. Device Manager is a tool that allows managing the hardware devices and drivers on a Windows workstation. System Configuration is a tool that allows modifying the startup options and services on a Windows workstation. None of these tools can directly grant administrator access to a user account. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13](#)

[CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103](#)

---

### Question: 328

---

An engineer is configuring a new server that requires a bare-metal installation. Which of the following installation methods should the engineer use if installation media is not available on site?

- A . Image deployment

- B . Recovery partition installation
- C . Remote network installation
- D . Repair installation

---

**Answer: C**

---

Explanation:

Remote network installation is the best option for configuring a new server that requires a bare-metal installation without installation media on site. A remote network installation is a method of installing an operating system or an application over a network connection, such as LAN, WAN, or Internet. A remote network installation can use various protocols, such as PXE, HTTP, FTP, or SMB, to access the installation files from a server or a cloud service. A remote network installation can also use various tools, such as Windows Deployment Services, Microsoft Deployment Toolkit, or Red Hat Kickstart, to automate and customize the installation process. A remote network installation can save time and resources by eliminating the need for physical media and allowing centralized management of multiple installations. Image deployment, recovery partition installation, and repair installation are not correct answers for this question. Image deployment is a method of installing an operating system or an application by copying a preconfigured image file to a target device. Image deployment requires an existing image file and a compatible device. Recovery partition installation is a method of restoring an operating system or an application from a hidden partition on the hard disk that contains the original factory settings. Recovery partition installation requires an existing recovery partition and a functional hard disk. Repair installation is a method of fixing an operating system or an application that is corrupted or damaged by replacing or repairing the system files without affecting the user data or settings. Repair installation requires an existing operating system or application and a working device. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 16](#)

[CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 106](#)

---

### **Question: 329**

---

A computer technician is investigating a computer that is not booting. The user reports that the computer was working prior to shutting it down last night. The technician notices a removable USB device is inserted, and the user explains the device is a prize the user received in the mail yesterday. Which of the following types of attacks does this describe?

- A . Phishing
- B . Dumpster diving
- C . Tailgating
- D . Evil twin

---

**Answer: A**

---

Explanation:

Phishing is the correct answer for this question. Phishing is a type of attack that uses fraudulent emails or other messages to trick users into revealing sensitive information or installing malicious software. Phishing emails often impersonate legitimate entities or individuals and offer incentives or threats to lure users into clicking on malicious links or attachments. In this scenario, the user received a removable USB device in the mail as a prize, which could be

a phishing attempt to infect the user's computer with malware or gain access to the user's data. Dumpster diving, tailgating, and evil twin are not correct answers for this question. Dumpster diving is a type of attack that involves searching through trash bins or recycling containers to find discarded documents or devices that contain valuable information. Tailgating is a type of attack that involves following an authorized person into a restricted area without proper identification or authorization. Evil twin is a type of attack that involves setting up a rogue wireless access point that mimics a legitimate one to intercept or manipulate network traffic. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25](#)

[CompTIA Security+ SY0-601 Certification Study Guide], page 1004

---

### Question: 330

---

A user is setting up backups on a workstation. The user wants to ensure that the restore process is as simple as possible. Which of the following backup types should the user select?

- A . Full
- B . Incremental
- C . Differential
- D . Synthetic

---

**Answer: A**

---

Explanation:

Full backup is the best option to ensure that the restore process is as simple as possible. A full backup is a backup type that copies all the data from the source to the destination, regardless of whether the data has changed or not. A full backup provides the most complete and consistent backup of the data, and it allows the user to restore the data from a single backup set without relying on any previous or subsequent backups. Incremental, differential, and synthetic backups are not as simple as full backups for restoring data. An incremental backup is a backup type that copies only the data that has changed since the last backup, whether it was full or incremental. An incremental backup requires less time and space than a full backup, but it also requires multiple backup sets to restore the data completely. A differential backup is a backup type that copies only the data that has changed since the last full backup. A differential backup requires more time and space than an incremental backup, but it also requires fewer backup sets to restore the data than an incremental backup. A synthetic backup is a backup type that combines a full backup with one or more incremental or differential backups to create a consolidated backup set. A synthetic backup requires less time and bandwidth than a full backup, but it also requires more processing power and storage space than an incremental or differential backup. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Cert Guide, page 458](#)

---

### Question: 331

---

A technician is partitioning a hard disk. The five primary partitions should contain 4TB of free space. Which of the following partition styles should the technician use to partition the device?

- A . EFS
- B . GPT
- C . MBR
- D . FAT32

---

**Answer: B**

---

Explanation:

GPT is the correct answer for this question. GPT stands for GUID Partition Table, and it is a partition style that supports up to 128 primary partitions and up to 18 exabytes of disk size per partition. GPT also uses a unique identifier for each partition and provides better data protection and recovery. GPT is suitable for partitioning a hard disk that has five primary partitions with 4TB of free space each. EFS, MBR, and FAT32 are not correct answers for this question. EFS stands for Encrypting File System, and it is a feature that allows encrypting files and folders on NTFS volumes. EFS is not a partition style, but rather a file system attribute. MBR stands for Master Boot Record, and it is an older partition style that supports up to four primary partitions and up to 2TB of disk size per partition. MBR cannot handle five primary partitions with 4TB of free space each. FAT32 stands for File Allocation Table 32, and it is a file system that supports up to 32GB of disk size per partition and up to 4GB of file size. FAT32 is not a partition style, but rather a file system type. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14](#)

[CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105](#)

---

### **Question: 332**

---

Which of the following would allow physical access to a restricted area while maintaining a record of events?

- A . Hard token
- B . Access control vestibule
- C . Key fob
- D . Door Lock

---

**Answer: B**

---

Explanation:

Access control vestibule is the correct answer for this question. An access control vestibule is a physical security device that consists of two doors that form an enclosed space between them. The first door opens only after verifying the identity of the person entering, such as by using a card reader, biometric scanner, or keypad. The second door opens only after the first door closes, creating a buffer zone that prevents unauthorized access or tailgating. An access control vestibule also maintains a record of events, such as who entered or exited, when, and how. Hard token, key fob, and door lock are not sufficient to meet the requirements of this question. A hard token is a device that generates a one-time password or code for authentication purposes. A key fob is a small device that can

be attached to a key ring and used to unlock doors or start vehicles remotely. A door lock is a mechanism that secures a door from opening without a key or a code. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25](#)

---

### Question: 333

---

A systems administrator is troubleshooting network performance issues in a large corporate office. The end users report that traffic to certain internal environments is not stable and often drops. Which of the following command-line tools can provide the most detailed information for investigating the issue further?

- A . ipconfig
- B . arp
- C . nslookup
- D . pathping

---

**Answer: D**

---

Explanation:

Pathping is the best command-line tool to provide the most detailed information for investigating the network performance issue further. Pathping is a utility that combines the functions of ping and tracert, which are two other command-line tools that test network connectivity and latency. Pathping sends packets to each router on the path to a destination and then computes results based on the packets returned from each hop. Pathping can show the route taken by the packets, the number of hops, the latency of each hop, and the packet loss percentage. This information can help the systems administrator identify where the network problem occurs and how severe it is. Ipconfig, arp, and nslookup are not as useful as pathping for this task. Ipconfig shows the configuration of the network interface card, such as IP address, subnet mask, and default gateway. Arp shows the mapping of IP addresses to MAC addresses in the local network. Nslookup queries DNS servers for domain name resolution. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 21](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Cert Guide, page 457](#)

---

### Question: 334

---

A large university wants to equip all classrooms with high-definition IP videoconferencing equipment. Which of the following would most likely be impacted in this situation?

- A . SAN
- B . LAN
- C . GPU
- D . PAN

---

**Answer: B**

---

## Explanation:

LAN is the most likely option to be impacted in this situation. LAN stands for Local Area Network, and it is a network that connects devices within a limited area, such as a building or a campus. Installing high-definition IP videoconferencing equipment in all classrooms would require a high bandwidth and reliable LAN infrastructure to support the video and audio transmission. The LAN would also need to be configured with proper security, quality of service, and multicast protocols to ensure the optimal performance of the videoconferencing system. SAN, GPU, and PAN are not directly related to this scenario. SAN stands for Storage Area Network, and it is a network that provides access to consolidated storage devices. GPU stands for Graphics Processing Unit, and it is a hardware component that handles graphics rendering and computation. PAN stands for Personal Area Network, and it is a network that connects devices within a short range, such as Bluetooth or infrared. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 20](#)

[CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 104](#)

Topic 5, Exam Pool E

---

## Question: 335

---

Which of the following is an advantage of using WPA2 instead of WPA3?

- A . Connection security
- B . Encryption key length
- C . Device compatibility
- D . Offline decryption resistance

---

**Answer: C**

---

## Explanation:

Device compatibility is an advantage of using WPA2 instead of WPA3. WPA2 is the previous version of the Wi-Fi Protected Access protocol, which provides security and encryption for wireless networks. WPA3 is the latest version, which offers improved security features, such as stronger encryption, enhanced protection against brute-force attacks, and easier configuration. However, WPA3 is not backward compatible with older devices that only support WPA2 or earlier protocols. Therefore, using WPA3 may limit the range of devices that can connect to the wireless network. Connection security, encryption key length, and offline decryption resistance are advantages of using WPA3 instead of WPA2. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 24](#)

[CompTIA A+ Certification All-in-One Exam Guide \(Exams 220-1101 & ..., page 1000](#)

---

## Question: 336

---

A technician is working on a Windows 10 PC that has unwanted applications starting on boot. Which of the following tools should the technician use to disable applications on startup?

- A . System Configuration
- B . Task Manager
- C . Performance Monitor
- D . Group Policy Editor

---

**Answer: B**

---

Explanation:

Task Manager is the best tool to use to disable applications on startup in Windows 10. Task Manager is a built-in utility that shows the current processes, performance, and users on a system. It also has a Startup tab that lists the applications that run on boot and their impact on the system. The technician can use Task Manager to disable or enable any application on startup by right-clicking on it and selecting the appropriate option. System Configuration, Performance Monitor, and Group Policy Editor are other tools that can be used to manage system settings, but they are not as simple or convenient as Task Manager for this task. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13](#)

[CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103](#)

---

### Question: 337

---

A technician is investigating options to secure a small office's wireless network. One requirement is to allow automatic log-ins to the network using certificates instead of passwords. Which of the following should the wireless solution have in order to support this feature?

- A . RADIUS
- B . AES
- C . EAP-EKE
- D . MFA

---

**Answer: A**

---

Explanation:

RADIUS is the correct answer for this question. RADIUS stands for Remote Authentication Dial-In User Service, and it is a protocol that provides centralized authentication, authorization, and accounting for wireless networks. RADIUS can support certificate-based authentication, which allows users to log in to the network automatically without entering passwords. RADIUS also provides other benefits, such as enforcing security policies, logging user activities, and managing network access. AES, EAP-EKE, and MFA are not wireless solutions, but rather encryption algorithms, authentication methods, and security factors, respectively. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 23](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Cert Guide, page 459](#)

---

### **Question: 338**

---

A remote user is experiencing issues connecting to a corporate email account on a laptop. The user clicks the internet connection icon and does not recognize the connected Wi-Fi. The help desk technician, who is troubleshooting the issue, assumes this is a rogue access point. Which of the following is the first action the technician should take?

- A . Restart the wireless adapter.
- B . Launch the browser to see if it redirects to an unknown site.
- C . Instruct the user to disconnect the Wi-Fi.
- D . Instruct the user to run the installed antivirus software.

---

**Answer: C**

---

Explanation:

Instructing the user to disconnect the Wi-Fi is the first action the technician should take if they suspect a rogue access point. A rogue access point is an unauthorized wireless network that could be used to intercept or manipulate network traffic, compromise security, or launch attacks. Disconnecting the Wi-Fi would prevent further exposure or damage to the user's device or data. Restarting the wireless adapter, launching the browser, or running the antivirus software are possible actions to take after disconnecting the Wi-Fi, but they are not as urgent or effective as the first step. Reference:

[Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 22](#)

[CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Cert Guide, page 456](#)

---

### **Question: 339**

---

A company's assets are scanned annually. Which of the following will most likely help the company gain a holistic view of asset cost?

- A . Creating a database
- B . Assigning users to assets
- C . Inventorying asset tags
- D . Updating the procurement account owners

---

**Answer: A**

---

Explanation:

Creating a database is the most likely option to help the company gain a holistic view of asset cost. A database can store and organize information about the assets, such as purchase date, depreciation value, maintenance cost, warranty status, and replacement cost. Assigning users to assets, inventorying asset tags, and updating the procurement account owners are important steps for asset management, but they do not directly provide a holistic view of asset cost. Reference:

---

### Question: 340

---

A customer is accessing a public kiosk in a company's lobby. Which of the following should be enforced to mitigate the risk of customer data being accidentally saved to the kiosk?

- A . Manually clearing browsing data
- B . Private-browsing mode
- C . Browser data synchronization
- D . Password manager

---

**Answer: B**

---

Explanation:

Private-browsing mode is the best option to mitigate the risk of customer data being accidentally saved to the kiosk. Private-browsing mode prevents the browser from storing cookies, history, passwords, and other data that could reveal the customer's identity or preferences. Manually clearing browsing data is not a reliable option, as it depends on the customer's awareness and willingness to do so. Browser data synchronization and password manager are features that could actually increase the risk of customer data being exposed, as they could sync or autofill sensitive information across devices or accounts. Reference:

---

### Question: 341

---

A user connected a smartphone to a coffee shop's public Wi-Fi and noticed the smartphone started sending unusual SMS messages and registering strange network activity. A technician thinks a virus or other malware has infected the device. Which of the following should the technician suggest the user do to best address these security and privacy concerns? (Select two).

- A . Disable Wi-Fi autoconnect.
- B . Stay offline when in public places.
- C . Uninstall all recently installed applications.
- D . Schedule an antivirus scan.
- E . Reboot the device
- F . Update the OS

---

**Answer: C, D**

---

### Explanation:

The best way to address the security and privacy concerns caused by a malware infection on a smartphone is to uninstall all recently installed applications and schedule an antivirus scan. Uninstalling the applications that may have introduced the malware can help remove the source of infection and prevent further damage. Scheduling an antivirus scan can help detect and remove any remaining traces of malware and restore the device's functionality.

---

### Question: 342

---

A payroll workstation has data on it that needs to be readily available and can be recovered quickly if something is accidentally removed. Which of the following backup methods should be used to provide fast data recovery in this situation?

- A . Full
- B . Differential
- C . Synthetic
- D . Incremental

---

**Answer: A**

---

### Explanation:

A full backup does not depend on any previous backups, unlike differential or incremental backups, which only save the changes made since the last backup. A synthetic backup is a type of full backup that combines an existing full backup with incremental backups to create a new full backup, but it still requires multiple backup sets to recover data.

a. [Therefore, a full backup is the most suitable for the payroll workstation that needs to have its data readily available and recoverable. You can learn more about the differences between full, differential, incremental, and synthetic backups from this article.](#)

---

### Question: 343

---

A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

- A . Document the date and time of the change.
- B . Submit a change request form.
- C . Determine the risk level of this change.
- D . Request an unused IP address.

---

**Answer: B**

---

### Explanation:

A change request form is a document that describes the proposed change, the reason for the change, the impact of the change, and the approval process for the change. A change request form is required for any planned changes to the network, such as adding a new network printer, to ensure that the change is authorized, documented, and communicated to all stakeholders. Submitting a change request form should happen immediately before network use is authorized, as stated in the Official CompTIA A+ Core 2 Study Guide. The other options are either too late (documenting the date and time of the change) or too early (determining the risk level of the change and requesting an unused IP address) in the change management process.

---

### Question: 344

---

During a network outage, a technician discovers a new network switch that was not listed in the support documentation. The switch was installed during a recent change window when a new office was added to the environment. Which of the following would most likely prevent this type of mismatch after next month's change window?

- A . Performing annual network topology reviews
- B . Requiring all network changes include updating the network diagrams
- C . Allowing network changes once per year
- D . Routinely backing up switch configuration files

---

### Answer: B

---

Explanation:

This would ensure that the support documentation reflects the current state of the network and prevents any confusion or mismatch during a network outage. Updating the network diagrams is also one of the best practices for network documentation, as stated in the Official CompTIA A+ Core 2 Study Guide1. The other options are not as effective or feasible as option B. Performing annual network topology reviews is too infrequent and may not capture recent changes. Allowing network changes once per year is too restrictive and may not meet the business needs. Routinely backing up switch configuration files is important, but it does not help with identifying new switches or devices on the network.

---

### Question: 345

---

A PC is taking a long time to boot. Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

- A . Installing additional RAM
- B . Removing the applications from startup
- C . Installing a faster SSD
- D . Running the Disk Cleanup utility
- E . Defragmenting the hard drive
- F . Ending the processes in the Task Manager

---

### Answer: B, E

---

## Explanation:

The correct answers are B) Removing the applications from startup and E. Defragmenting the hard drive. These are the operations that would be best to do to resolve the issue of a slow boot at a minimal expense.

Removing the applications from startup means disabling the programs that run automatically when the PC is turned on. This will reduce the load on the CPU and RAM and speed up the boot process1.

Defragmenting the hard drive means rearranging the files on the disk so that they are stored in contiguous blocks. This will improve the disk performance and reduce the time it takes to read and write data2.

1: CompTIA A+ Certification Exam: Core 2 Objectives, page 23, section 3.1. 2: CompTIA A+ Certification Exam: Core 2 Objectives, page 24, section 3.2.

---

## Question: 346

---

A technician is unable to access the internet or named network resources. The technician receives a valid IP address from the DHCP server and can ping the default gateway. Which of the following should the technician check next to resolve the issue?

- A . Verify the DNS server settings.
- B . Turn off the Windows firewall.
- C . Confirm the subnet mask is correct.
- D . Configure a static IP address.

---

**Answer: A**

---

## Explanation:

The correct answer is

A) Verify the DNS server settings. This is because the DNS server is responsible for resolving domain names to IP addresses, which is necessary for accessing the internet or named network resources. If the DNS server settings are incorrect or the DNS server is down, the technician will not be able to access these resources even if they have a valid IP address and can ping the default gateway1.

1: CompTIA A+ Certification Exam: Core 2 Objectives, page 16, section 1.10.

---

## Question: 347

---

A company recently outsourced its night-shift cleaning service. A technician is concerned about having unsupervised contractors in the building. Which of the following security measures can be used to prevent the computers from being accessed? (Select two).

- A . Implementing data-at-rest encryption
- B . Disabling AutoRun

- C . Restricting user permissions
- D . Restricting log-in times
- E . Enabling a screen lock
- F . Disabling local administrator accounts

---

**Answer: D, E**

---

Explanation:

The correct answers are D. Restricting log-in times and E. Enabling a screen lock. These are the security measures that can be used to prevent the computers from being accessed by unsupervised contractors in the building.

Restricting log-in times means setting a policy that allows users to log in only during certain hours, such as the regular working hours of the company. This will prevent unauthorized access by contractors who work at night1.

Enabling a screen lock means setting a policy that requires users to enter a password or a PIN to unlock their screens after a period of inactivity. This will prevent unauthorized access by contractors who might try to use the computers when the users are away2.

[1: CompTIA A+ Certification Exam: Core 2 Objectives, page 19, section 2.3.](#) [2: CompTIA A+ Certification Exam: Core 2 Objectives, page 20, section 2.4.](#)

---

### **Question: 348**

---

A customer has a USB-only printer attached to a computer. A technician is configuring an arrangement that allows other computers on the network to use the printer. In which of the following locations on the customer's desktop should the technician make this configuration?

- A . Printing Preferences/Advanced tab
- B . Printer Properties/Sharing tab
- C . Printer Properties/Security tab
- D . Printer Properties/Ports tab

---

**Answer: B**

---

Explanation:

The correct answer is B. Printer Properties/Sharing tab. This is the location where the technician can enable printer sharing and assign a share name for the USB printer. This will allow other computers on the network to access the printer by using the share name or the IP address of the computer that has the printer attached1.

[1: CompTIA A+ Certification Exam: Core 2 Objectives, page 15, section 1.9.](#)

---

### **Question: 349**

---

A workstation is displaying a message indicating that a user must exchange cryptocurrency for a decryption key. Which of the following is the best way for a technician to return the device to service safely?

- A . Run an AV scan.
- B . Reinstall the operating system
- C . Install a software firewall.
- D . Perform a system restore.
- E . Comply with the on-screen instructions.

---

**Answer: B**

---

Explanation:

The best way for a technician to return the device to service safely is to reinstall the operating system. This is because the device is infected by ransomware, which is a form of malware that encrypts files and demands payment for decryption. Reinstalling the operating system will erase the ransomware and restore the device to its original state. However, this will also delete any data that was not backed up before the infection. Therefore, it is important to have regular backups of critical data and protect them from ransomware attacks1.

The other options are not effective or safe for ransomware recovery. Running an AV scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Installing a software firewall may prevent future attacks, but it will not help with the current infection. Performing a system restore may not work if the ransomware has corrupted or deleted the restore points. Complying with the on-screen instructions is not advisable, as it will encourage the attackers and there is no guarantee that they will provide the decryption key after receiving the payment.

To prevent and recover from ransomware attacks, it is recommended to follow some best practices, such as234:

Use strong passwords and multifactor authentication for all accounts and devices.

Keep all software and firmware updated with the latest security patches.

Avoid opening suspicious or unsolicited emails and attachments.

Educate users and staff on how to recognize and report phishing and social engineering attempts.

Use antivirus software and enable real-time protection.

Enable network segmentation and firewall rules to limit the spread of ransomware.

Implement a Zero Trust security model to verify all requests and devices before granting access.

Create and test backups of critical data and store them offline or in a separate network.

Recover safely by isolating the infected devices, identifying the ransomware variant, and restoring data from backups.

Report any ransomware incidents to law enforcement agencies and seek help from experts.

---

**Question: 350**

---

A remote user is experiencing issues with Outlook settings and asks a technician to review the settings. Which of the following can the technician use to access the user's computer remotely?

- A . VPN
- B . RDP
- C . RMM
- D . SSH

---

**Answer: B**

---

Explanation:

One of the possible ways to access the user's computer remotely is to use RDP, which stands for Remote Desktop Protocol. RDP is a protocol that allows a user to connect to another computer over a network and use its graphical interface. RDP is commonly used for remote desktop software, such as Microsoft Remote Desktop Connection1. To use RDP, the user's computer must run RDP server software, and the technician must run RDP client software. The technician can then enter the user's IP address or hostname, and provide the appropriate credentials to log in to the user's computer. Once connected, the technician can view and control the user's desktop, and review the Outlook settings.

---

### **Question: 351**

---

Users access files in the department share. When a user creates a new subfolder, only that user can access the folder and its files. Which of the following will MOST likely allow all users to access the new folders?

- A . Assigning share permissions
- B . Enabling inheritance
- C . Requiring multifactor authentication
- D . Removing archive attribute

---

**Answer: B**

---

Explanation:

Enabling inheritance is a method that allows new subfolders to inherit the permissions and settings from their parent folder. If users can access files in the department share, but not in the new subfolders created by other users, it may indicate that inheritance is disabled and that each new subfolder has its own permissions and settings that restrict access to only the creator. Enabling inheritance can help resolve this issue by allowing all users to access the new subfolders with the same permissions and settings as the department share. Assigning share permissions, requiring multifactor authentication, and removing archive attribute are not methods that can most likely allow all users to access the new folders.

---

### **Question: 352**

---

Which of the following threats will the use of a privacy screen on a computer help prevent?

- A . Impersonation
- B . Shoulder surfing
- C . Whaling
- D . Tailgating

---

**Answer: B**

---

Explanation:

Shoulder surfing is a threat that involves someone looking over another person's shoulder to observe their screen, keyboard, or other sensitive information. Shoulder surfing can be used to steal passwords, personal identification numbers (PINs), credit card numbers, or other confidential data. The use of a privacy screen on a computer can help prevent shoulder surfing by limiting the viewing angle of the screen and making it harder for someone to see the screen from the side or behind. Impersonation, whaling, and tailgating are not threats that can be prevented by using a privacy screen on a computer.

---

### **Question: 353**

---

An administrator responded to an incident where an employee copied financial data to a portable hard drive and then left the company with the data

a. The administrator documented the movement of the evidence. Which of the following concepts did the administrator demonstrate?

- A . Preserving chain of custody
- B . Implementing data protection policies
- C . Informing law enforcement
- D . Creating a summary of the incident

---

**Answer: A**

---

Explanation:

Preserving chain of custody is a concept that refers to the documentation and tracking of who handled, accessed, modified, or transferred a piece of evidence, when, where, why, and how. Preserving chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. An administrator who documented the movement of the evidence demonstrated the concept of preserving chain of custody. Implementing data protection policies, informing law enforcement, and creating a summary of the incident are not concepts that describe the action of documenting the movement of the evidence.

---

### **Question: 354**

---

A user visits a game vendor's website to view the latest patch notes, but this information is not available on the page. Which of the following should the user perform before reloading the page?

- A . Synchronize the browser data.
- B . Enable private browsing mode.
- C . Mark the site as trusted.
- D . Clear the cached file.

---

**Answer: D**

---

Explanation:

Clearing the cached file is an action that can help resolve the issue of not seeing the latest patch notes on a game vendor's website. A cached file is a copy of a web page or file that is stored locally on the user's browser or device for faster loading and offline access. However, sometimes a cached file may become outdated or corrupted and prevent the user from seeing the most recent or accurate version of a web page or file. Clearing the cached file can force the browser to download and display the latest version from the server instead of using the old copy from the cache. Synchronizing the browser data, enabling private browsing mode, and marking the site as trusted are not actions that can help resolve this issue.

---

### **Question: 355**

---

Which of the following allows access to the command line in macOS?

- A . PsExec
- B . command.com
- C . Terminal
- D . CMD

---

**Answer: C**

---

Explanation:

Terminal is an application that allows access to the command line in macOS. The command line is an interface that allows users to interact with the operating system and perform various tasks by typing commands and arguments. Terminal can be used to launch programs, manage files and folders, configure settings, troubleshoot issues, and run scripts in macOS. PsExec, command.com, and CMD are not applications that allow access to the command line in macOS.

---

### **Question: 356**

---

A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company's requirements?

- A . Biometrics
- B . Soft token
- C . Access control lists
- D . Smart card

Explanation:

A soft token, also known as a software token or an OTP (one-time password) app, is a type of multifactor authentication that generates a temporary code or password on a user's device, such as a smartphone or a tablet. The user must enter this code or password along with their username and password to access their account or service. A soft token can help improve security by adding an extra layer of verification and preventing unauthorized access even if the user's credentials are compromised. A soft token can also be implemented at a minimal cost, as it does not require any additional hardware or infrastructure. Biometrics, access control lists, and smart card are not types of multifactor authentication that can be implemented at a minimal cost.

---

**Question: 357**

---

A user installed a new computer game. Upon starting the game, the user notices the frame rates are low. Which of the following should the user upgrade to resolve the issue?

- A . Hard drive
- B . Graphics card
- C . Random-access memory
- D . Monitor

Explanation:

A graphics card, also known as a video card or a GPU (graphics processing unit), is a component that can affect the performance of a computer game. A graphics card is responsible for rendering and displaying graphics on the screen, such as images, animations, and effects. A computer game may require a high level of graphics processing power to run smoothly and achieve high frame rates, which are the number of frames per second (FPS) that the game can display. Upgrading to a better graphics card can improve the performance of a computer game by increasing its graphics quality and frame rates. Hard drive, random-access memory, and monitor are not components that can directly improve the performance of a computer game.

---

**Question: 358**

---

Which of the following helps ensure that a piece of evidence extracted from a PC is admissible in a court of law?

- A . Data integrity form
- B . Valid operating system license
- C . Documentation of an incident
- D . Chain of custody

---

**Answer: D**

---

Explanation:

Chain of custody is a process that helps ensure that a piece of evidence extracted from a PC is admissible in a court of law. Chain of custody refers to the documentation and tracking of who handled, accessed, modified, or transferred the evidence, when, where, why, and how. Chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. Data integrity form, valid operating system license, and documentation of an incident are not processes that can ensure that a piece of evidence extracted from a PC is admissible in a court of law.

---

### **Question: 359**

---

A help desk technician determines a motherboard has failed. Which of the following is the most logical next step in the remediation process?

- A . Escalating the issue to Tier 2
- B . Verifying warranty status with the vendor
- C . Replacing the motherboard
- D . Purchasing another PC

---

**Answer: B**

---

Explanation:

Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a guarantee from the vendor that covers the repair or replacement of defective or faulty products within a specified period of time. Verifying warranty status with the vendor can help the technician determine if the motherboard is eligible for warranty service and what steps to take to obtain it. Escalating the issue to Tier 2, replacing the motherboard, and purchasing another PC are not the most logical next steps in the remediation process.

---

### **Question: 360**

---

A company is experiencing a DDoS attack. Several internal workstations are the source of the traffic. Which of the following types of infections are the workstations most likely experiencing? (Select two).

- A . Zombies
- B . Keylogger
- C . Adware
- D . Botnet
- E . Ransomware
- F . Spyware

---

**Answer: A, D**

---

Explanation:

Zombies and botnets are terms that describe the types of infections that can cause internal workstations to participate in a DDoS (distributed denial-of-service) attack. A DDoS attack is a malicious attempt to disrupt the normal functioning of a website or a network by overwhelming it with a large amount of traffic from multiple sources. Zombies are infected computers that are remotely controlled by hackers without the owners' knowledge or consent. Botnets are networks of zombies that are coordinated by hackers to launch DDoS attacks or other malicious activities. Keylogger, adware, ransomware, and spyware are not types of infections that can cause internal workstations to participate in a DDoS attack.

---

### **Question: 361**

---

Which of the following would most likely be used to extend the life of a device?

- A . Battery backup
- B . Electrostatic discharge mat
- C . Proper ventilation
- D . Green disposal

---

**Answer: C**

---

Explanation:

Proper ventilation is a factor that can extend the life of a device by preventing overheating and thermal damage to the device's components. Proper ventilation means ensuring that there is enough airflow around and inside the device to dissipate heat and maintain a suitable temperature for optimal performance. Proper ventilation can be achieved by using fans, heat sinks, vents, or liquid cooling systems, as well as avoiding placing the device near heat sources or in enclosed spaces. Battery backup, electrostatic discharge mat, and green disposal are not factors that can extend the life of a device.

---

### **Question: 362**

---

The screen on a user's mobile device is not autorotating even after the feature has been enabled and the device has been restarted. Which of the following should the technician do next to troubleshoot the issue?

- A . Calibrate the phone sensors.
- B . Enable the touch screen.
- C . Reinstall the operating system.
- D . Replace the screen.

---

**Answer: A**

---

## Explanation:

Calibrating the phone sensors is a step that can troubleshoot the issue of screen not autorotating on a mobile device. Screen autorotation is a feature that automatically adjusts the screen orientation based on the device's position and movement. Screen autorotation relies on sensors such as accelerometer and gyroscope to detect the device's tilt and rotation. Calibrating the phone sensors can help fix any errors or inaccuracies in the sensor readings that may prevent screen autorotation from working properly. Enabling the touch screen, reinstalling the operating system, and replacing the screen are not steps that should be done next to troubleshoot this issue.

---

### Question: 363

---

A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

- A . Factory reset
- B . System Restore
- C . In-place upgrade
- D . Unattended installation

---

**Answer: D**

---

## Explanation:

An unattended installation is a method of installing Windows 10 that does not require any user input or interaction during the installation process. An unattended installation can be performed by using an answer file, which is a file that contains all the configuration settings and preferences for the installation, such as the product key, the language, the partition size, and the user accounts. An unattended installation can be the fastest way to install Windows 10, as it automates and streamlines the installation process. Factory reset, System Restore, and in-place upgrade are not methods of installing Windows 10.

---

### Question: 364

---

During an enterprise rollout of a new application, a technician needs to validate compliance with an application's EULA while also reducing the number of licenses to manage. Which of the following licenses would best accomplish this goal?

- A . Personal use license
- B . Corporate use license
- C . Open-source license
- D . Non-expiring license

---

**Answer: B**

---

## Explanation:

A corporate use license, also known as a volume license, is a type of software license that allows an organization to purchase and use multiple copies of a software product with a single license key. A corporate use license can help validate compliance with an application's EULA (end-user license agreement), which is a legal contract that defines the terms and conditions of using the software. A corporate use license can also reduce the number of licenses to manage, as it eliminates the need to activate and track individual licenses for each copy of the software. Personal use license, open-source license, and non-expiring license are not types of licenses that can best accomplish this goal.

---

### Question: 365

---

A PC is taking a long time to boot. Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

- A . Installing additional RAM
- B . Removing the applications from startup
- C . Installing a faster SSD
- D . Running the Disk Cleanup utility
- E . Defragmenting the hard drive
- F . Ending the processes in the Task Manager

---

**Answer: B, D**

---

Explanation:

Removing the applications from startup can improve the boot time of a PC by reducing the number of programs that load automatically when the PC starts. Some applications may add themselves to the startup list without the user's knowledge or consent, which can slow down the PC's performance. Running the Disk Cleanup utility can also improve the boot time of a PC by deleting unnecessary or temporary files that take up disk space and affect the PC's speed. Disk Cleanup can also remove old system files that may cause conflicts or errors during booting. Installing additional RAM, installing a faster SSD, defragmenting the hard drive, and ending the processes in the Task Manager are not operations that would be best to do to resolve the issue of slow boot time at a minimal expense, as they may require purchasing new hardware or software, or may have negative impacts on other aspects of the PC's performance.

---

### Question: 366

---

A technician needs to ensure that USB devices are not suspended by the operating system. Which of the following Control Panel utilities should the technician use to configure the setting?

- A . System
- B . Power Options
- C . Devices and Printers
- D . Ease of Access

---

**Answer: B**

---

## Explanation:

Power Options is a Control Panel utility that allows users to configure the power settings of their computer, such as when to turn off the display, when to put the computer to sleep, and how to manage the battery life. Power Options also allows users to configure the USB selective suspend setting, which is a feature that automatically suspends the power supply to USB devices that are not in use, in order to save energy. A user can disable this setting if they want to ensure that USB devices are not suspended by the operating system. System, Devices and Printers, and Ease of Access are not Control Panel utilities that can be used to configure the USB selective suspend setting.

---

### Question: 367

---

A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation. Which of the following actions should be taken to prevent this incident from happening again? (Select two).

- A . Install a host-based IDS.
- B . Restrict log-in times.
- C . Enable a BIOS password.
- D . Update the password complexity.
- E . Disable AutoRun.
- F . Update the antivirus definitions.
- G . Restrict user permissions.

---

**Answer: E, G**

---

## Explanation:

AutoRun is a feature of Windows that automatically executes a program or file when a removable media such as a USB drive is inserted into the computer. Disabling AutoRun can prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would require the user to manually open the drive and run the file. Restricting user permissions can also prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would limit the user's ability to execute or install unauthorized programs or files. Installing a host-based IDS, restricting log-in times, enabling a BIOS password, updating the password complexity, and updating the antivirus definitions are not actions that can directly prevent this incident from happening again.

---

### Question: 368

---

A Windows administrator is creating user profiles that will include home directories and network printers for several new users. Which of the following is the most efficient way for the technician to complete this task?

- A . Access control
- B . Authentication application
- C . Group Policy
- D . Folder redirection

---

**Answer: C**

---

Explanation:

Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain. Group Policy can be used to create user profiles that include home directories and network printers for several new users, as well as other configurations such as security settings, desktop preferences, and software installation. Group Policy can save time and effort for the administrator by applying the same settings to multiple users at once. Access control, authentication application, and folder redirection are not the most efficient ways to create user profiles that include home directories and network printers for several new users.

---

**Question: 369**

---

A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer; thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

- A . Document the date and time of the change.
- B . Submit a change request form.
- C . Determine the risk level of this change.
- D . Request an unused IP address.

---

**Answer: D**

---

Explanation:

An IP address is a unique identifier that allows a device to communicate with other devices on a network. A network printer needs an IP address to be accessible by multiple users on the network. Requesting an unused IP address from the network administrator or using an IP address scanner is the step that should happen immediately before network use is authorized, as it ensures that there is no IP address conflict or duplication on the network. Documenting the date and time of the change, submitting a change request form, and determining the risk level of this change are steps that should happen before requesting an unused IP address.

---

**Question: 370**

---

Which of the following would most likely be used in a small office environment?

- A . Print server
- B . Virtualization
- C . Domain access
- D . Workgroup

---

**Answer: D**

---

### **Explanation:**

A workgroup is a network configuration that allows computers to communicate and share resources with each other without requiring a centralized server or domain controller. A workgroup is suitable for small office environments where there are only a few computers and users who need simple file and printer sharing. A workgroup does not have centralized management or security policies, which may be desirable for larger or more complex networks. Print server, virtualization, and domain access are not network configurations that are most likely used in a small office environment.

---

### **Question: 371**

---

A user wants to back up a Windows 10 device. Which of the following should the user select?

- A . Devices and Printers
- B . Email and Accounts
- C . Update and Security
- D . Apps and Features

---

**Answer: C**

---

### **Explanation:**

Update and Security is the section in Windows 10 Settings that allows the user to back up their device. Backing up a device means creating a copy of the data and settings on the device and storing it in another location, such as an external drive or a cloud service. Backing up a device can help the user restore their data and settings in case of data loss, corruption, or theft. Devices and Printers, Email and Accounts, and Apps and Features are not sections in Windows 10 Settings that allow the user to back up their device.

---

### **Question: 372**

---

A desktop technician has received reports that a user's PC is slow to load programs and saved files. The technician investigates and discovers an older HDD with adequate free space. Which of the following should the technician use to alleviate the issue first?

- A . Disk Management
- B . Disk Defragment
- C . Disk Cleanup
- D . Device Manager

---

**Answer: B**

---

### **Explanation:**

Disk Defragment is a tool that can be used to improve the performance of a hard disk drive (HDD). HDDs store data in sectors and clusters on spinning platters. Over time, as data is written, deleted, and moved, the data may become fragmented, meaning that it is spread across different locations on the disk. This causes the HDD to take longer to access and load data, resulting in slower performance. Disk Defragment consolidates the fragmented data and rearranges it in a contiguous manner, which reduces the seek time and increases the speed of the HDD. Disk Management, Disk Cleanup, and Device Manager are not tools that can alleviate the issue of slow HDD performance.

---

### Question: 373

---

A user requires a drive to be mapped through a Windows command line. Which of the following command-line tools can be utilized to map the drive?

- A . gpupdate
- B . net use
- C . hostname
- D . dir

---

### Answer: B

---

Explanation:

Net use is a command-line tool that can be used to map a drive in Windows. Mapping a drive means assigning a drive letter to a network location or a local folder, which allows the user to access it more easily and quickly. Net use can also be used to disconnect a mapped drive, display information about mapped drives, or connect to shared resources on another computer. Gpupdate, hostname, and dir are not command-line tools that can be used to map a drive.

---

### Question: 374

---

A technician installs specialized software on a workstation. The technician then attempts to run the software. The workstation displays a message indicating the software is not authorized to run. Which of the following should the technician do to most likely resolve the issue?

- A . Install the software in safe mode.
- B . Attach the external hardware token.
- C . Install OS updates.
- D . Restart the workstation after installation.

---

### Answer: B

---

Explanation:

A hardware token is a physical device that provides an additional layer of security for software authorization. Some specialized software may require a hardware token to be attached to the workstation in order to run. A hardware token may contain a cryptographic key, a password, or a one-time code that verifies the user's identity or permission.

Installing the software in safe mode, installing OS updates, and restarting the workstation after installation are not likely to resolve the issue of software authorization.

---

### **Question: 375**

---

Which of the following best describes when to use the YUM command in Linux?

- A . To add functionality
- B . To change folder permissions
- C . To show documentation
- D . To list file contents

---

**Answer: A**

---

Explanation:

YUM stands for Yellowdog Updater Modified and it is a command-line tool that allows users to install, update, remove, and manage software packages in Linux. YUM can be used to add functionality to a Linux system by installing new software packages or updating existing ones. To change folder permissions, show documentation, or list file contents, other commands such as chmod, man, or ls can be used in Linux.

---

### **Question: 376**

---

A hard drive that previously contained PII needs to be repurposed for a public access workstation. Which of the following data destruction methods should a technician use to ensure data is completely removed from the hard drive?

- A . Shredding
- B . Degaussing
- C . Low-level formatting
- D . Recycling

---

**Answer: A**

---

Explanation:

Shredding is a data destruction method that physically destroys the hard drive by cutting it into small pieces using a machine. Shredding ensures that data is completely removed from the hard drive and cannot be recovered by any means. Shredding is suitable for hard drives that contain PII (personally identifiable information), which is any information that can be used to identify, contact, or locate an individual. Degaussing, low-level formatting, and recycling are not data destruction methods that can guarantee complete data removal from a hard drive.

---

### **Question: 377**

---

The battery life on an employee's new phone seems to be drastically less than expected, and the screen stays on for a very long time after the employee sets the phone down. Which of the following should the technician check first to troubleshoot this issue? (Select two).

- A . Screen resolution
- B . Screen zoom
- C . Screen timeout
- D . Screen brightness
- E . Screen damage
- F . Screen motion smoothness

---

**Answer: C, D**

---

Explanation:

Screen timeout is the setting that determines how long the screen stays on after the user stops interacting with the phone. Screen brightness is the setting that determines how much light the screen emits. Both of these settings affect the battery life of the phone, as keeping the screen on longer and brighter consumes more power than turning it off sooner and dimmer. A technician should check these settings first to troubleshoot the issue of low battery life and adjust them accordingly. Screen resolution, screen zoom, screen damage, and screen motion smoothness are not settings that directly affect the battery life or the screen staying on for a long time.

---

### **Question: 378**

---

A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?

- A . Battery backup
- B . Thermal paste
- C . ESD strap
- D . Consistent power

---

**Answer: C**

---

Explanation:

An ESD strap, also known as an antistatic wrist strap, is a device that prevents electrostatic discharge (ESD) from damaging sensitive electronic components such as RAM. ESD is the sudden flow of electricity between two objects with different electrical charges, which can cause permanent damage or malfunction to electronic devices. An ESD strap connects the technician's wrist to a grounded surface, such as a metal case or a mat, and equalizes the electrical potential between the technician and the device. Battery backup, thermal paste, and consistent power are not devices that can protect against ESD.

---

### **Question: 379**

---

A user contacts the help desk to request assistance with a program feature. The user is in a different building but on the same network as the help desk technician. Which of the following should the technician use to assist the user?

- A . AAA
- B . SSH
- C . RDP
- D . VPN

---

**Answer: C**

---

Explanation:

RDP stands for Remote Desktop Protocol and it is a protocol that allows a user to remotely access and control another computer over a network. A technician can use RDP to assist a user who is in a different building but on the same network by connecting to the user's computer and viewing their screen, keyboard, and mouse. AAA, SSH, and VPN are not protocols that can be used to assist a user with a program feature.

---

### **Question: 380**

---

A technician sees a file that is requesting payment to a cryptocurrency address. Which of the following should the technician do first?

- A . Quarantine the computer.
- B . Disable System Restore.
- C . Update the antivirus software definitions.
- D . Boot to safe mode.

---

**Answer: A**

---

Explanation:

Quarantining the computer means isolating it from the network and other devices to prevent the spread of malware or ransomware. Ransomware is a type of malware that encrypts the files on a computer and demands payment (usually in cryptocurrency) to restore them. If a technician sees a file that is requesting payment to a cryptocurrency address, it is likely that the computer has been infected by ransomware. Quarantining the computer should be the first step to contain the infection and prevent further damage. Disabling System Restore, updating the antivirus software definitions, and booting to safe mode are not steps that should be done before quarantining the computer.

---

### **Question: 381**

---

While trying to repair a Windows 10 OS, a technician receives a prompt asking for a key. The technician tries the administrator password, but it is rejected. Which of the following does the technician need in order to continue the OS repair?

- A . SSL key
- B . Preshared key
- C . WPA2 key
- D . Recovery key

---

**Answer: D**

---

Explanation:

A recovery key is a code that can be used to unlock a BitLocker-encrypted drive when the normal authentication methods (such as password or PIN) are not available or have been forgotten. BitLocker is a feature of Windows that encrypts the entire drive to protect data from unauthorized access. If a technician is trying to repair a Windows 10 OS that has BitLocker enabled, they will need the recovery key to access the drive and continue the OS repair. SSL key, preshared key, and WPA2 key are not keys that are related to BitLocker or OS repair.

---

### **Question: 382**

---

A technician is concerned about a large increase in the number of whaling attacks happening in the industry. The technician wants to limit the company's risk to avoid any issues. Which of the following items should the technician implement?

- A . Screened subnet
- B . Firewall
- C . Anti-phishing training
- D . Antivirus

---

**Answer: C**

---

Explanation:

Anti-phishing training is a method of educating users on how to identify and avoid phishing attacks, which are attempts to trick users into revealing sensitive information or performing malicious actions by impersonating legitimate entities or persons. Whaling attacks are a specific type of phishing attack that target high-level executives or influential individuals within an organization. Anti-phishing training can help users recognize the signs of whaling attacks and prevent them from falling victim to them. Screened subnet, firewall, and antivirus are not items that can directly address the issue of whaling attacks.

---

### **Question: 383**

---

A user connected an external hard drive but is unable to see it as a destination to save files. Which of the following tools will allow the drive to be formatted?

- A . Disk Management
- B . Device Manager
- C . Disk Cleanup

D . Disk Defragmenter

---

**Answer: A**

---

Explanation:

Disk Management is a tool that allows users to create, format, delete, shrink, extend, and manage partitions on hard drives. If the external hard drive is not formatted or has an incompatible filesystem type, Disk Management can be used to format it with a supported filesystem type such as NTFS, FAT32, or exFAT. Device Manager, Disk Cleanup, and Disk Defragmenter are not tools that can format a hard drive.

---

### **Question: 384**

---

A systems administrator is configuring centralized desktop management for computers on a domain. The management team has decided that all users' workstations should have the same network drives, printers, and configurations. Which of the following should the administrator use to accomplish this task?

- A . Network and Sharing Center
- B . net use
- C . User Accounts
- D . regedit
- E . Group Policy

---

**Answer: E**

---

Explanation:

Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain. Group Policy can be used to configure network drives, printers, security settings, desktop preferences, and other configurations for all users' workstations. Network and Sharing Center, net use, User Accounts, and regedit are not tools that can accomplish this task.

---

### **Question: 385**

---

A user is unable to access several documents saved on a work PC. A technician discovers the files were corrupted and must change several system settings within Registry Editor to correct the issue. Which of the following should the technician do before modifying the registry keys?

- A . Update the anti-malware software.
- B . Create a restore point.
- C . Run the PC in safe mode.
- D . Roll back the system updates.

---

**Answer: B**

---

Explanation:

A restore point is a snapshot of the system settings and configuration at a specific point in time<sup>2</sup>. Creating a restore point before modifying the registry keys allows the technician to revert the system back to a previous state if something goes wrong or causes instability<sup>2</sup>. Updating the anti-malware software, running the PC in safe mode, and rolling back the system updates are not necessary steps before modifying the registry keys.

---

### Question: 386

---

Which of the following filesystem types does macOS use?

- A . ext4
- B . exFAT
- C . NTFS
- D . APFS

---

**Answer: D**

---

Explanation:

APFS stands for Apple File System and it is the default filesystem type for macOS since High Sierra (10.13)<sup>1</sup>. APFS is optimized for flash storage and supports features such as encryption, snapshots, cloning, and space sharing<sup>1</sup>.

---

### Question: 387

---

A technician needs to ensure that USB devices are not suspended by the operating system. Which of the following Control Panel utilities should the technician use to configure the setting?

- A . System
- B . Power Options
- C . Devices and Printers
- D . Ease of Access

---

**Answer: B**

---

Explanation:

The correct answer is B) Power Options. The Power Options utility in the Control Panel allows you to configure various settings related to how your computer uses and saves power, such as the power plan, the sleep mode, the screen brightness, and the battery status. To access the Power Options utility, you can follow these steps:

Go to Control Panel > Hardware and Sound > Power Options.

Click on Change plan settings for the power plan you are using.

Click on Change advanced power settings.

Expand the USB settings category and then the USB selective suspend setting subcategory.

Set the option to Disabled for both On battery and Plugged in.

Click on OK and then on Save changes.

This will prevent the operating system from suspending the USB devices to save power .

System, Devices and Printers, and Ease of Access are not the utilities that should be used to configure the setting. System is a utility that provides information about your computer's hardware and software, such as the processor, memory, operating system, device manager, and system protection. Devices and Printers is a utility that allows you to view and manage the devices and printers connected to your computer, such as adding or removing devices, changing device settings, or troubleshooting problems. Ease of Access is a utility that allows you to customize your computer's accessibility options, such as the narrator, magnifier, high contrast, keyboard, mouse, and speech recognition. None of these utilities have any option to configure the USB selective suspend setting.

---

### Question: 388

---

A new employee is having difficulties using a laptop with a docking station. The laptop is connected to the docking station, and the laptop is closed. The external monitor works for a few seconds, but then the laptop goes to sleep. Which of the following options should the technician configure in order to fix the issue?

- A . Hibernate
- B . Sleep/suspend
- C . Choose what closing the lid does
- D . Turn on fast startup

---

**Answer: C**

---

Explanation:

The correct answer is C) Choose what closing the lid does. This option allows you to configure how the laptop behaves when you close the lid, such as whether it goes to sleep, hibernates, shuts down, or does nothing. To access this option, you can follow these steps :

Go to Settings > System > Power & sleep.

Click on Additional power settings on the right side.

Click on Choose what closing the lid does on the left side.

Under When I close the lid, select Do nothing for both On battery and Plugged in.

Click on Save changes.

This will prevent the laptop from going to sleep when you close the lid while it is connected to the docking station and the external monitor.

Hibernate, sleep/suspend, and turn on fast startup are not the options that should be configured to fix the issue. Hibernate and sleep/suspend are both power-saving modes that allow you to resume your work without losing any data.

a. However, they also turn off the display and other components of the laptop, which means you will not be able to use the external monitor when the laptop is closed. Turn on fast startup is a feature that reduces the boot time of Windows by saving some system information to a file when you shut down. It does not affect how the laptop behaves when you close the lid.

---

### Question: 389

---

A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation. Which of the following actions should be taken to prevent this incident from happening again? (Select two).

- A . Install a host-based IDS
- B . Restrict log-in times.
- C . Enable a BIOS password
- D . Update the password complexity
- E . Disable AutoRun.
- F . Update the antivirus definitions.
- G . Restrict user permissions.

---

**Answer: E, F**

---

Explanation:

The correct answers are E and F) Disabling AutoRun and updating the antivirus definitions are two actions that should be taken to prevent the incident from happening again.

AutoRun is a feature of Windows that automatically executes a predetermined action when a removable media such as a USB drive is inserted in a computer. For example, AutoRun can launch or install a new program on the media, or open the file in File Explorer. However, this feature can also be exploited by malicious software that can run without the user's consent or knowledge. Therefore, disabling AutoRun can help prevent accidental installation of viruses and other malware from USB drives123.

Updating the antivirus definitions is another important action that can help prevent malware infections from USB drives. Antivirus definitions are files that contain information about the latest known threats and how to detect and remove them. By updating the antivirus definitions regularly, you can ensure that your antivirus software can recognize and block any malicious software that may be on the USB drive before it can harm your computer45.

A host-based IDS is a system that monitors and analyzes the activity on a single computer or device for any signs of intrusion or malicious behavior. A host-based IDS can help detect and prevent malware infections from USB drives, but it is not a sufficient action by itself. A host-based IDS needs to be complemented by other security measures, such as disabling AutoRun and updating the antivirus definitions6.

Restricting login times, enabling a BIOS password, and updating the password complexity are all actions that can help improve the security of a computer or device, but they are not directly related to preventing malware infections from USB drives. These actions can help prevent unauthorized access to the computer or device, but they do not affect how the computer or device interacts with the USB drive or its contents.

Restricting user permissions is an action that can help limit the damage that malware can cause on a computer or device, but it does not prevent the malware from being installed in the first place. Restricting user permissions means limiting what actions a user can perform on the computer or device, such as installing or deleting programs, modifying system settings, or accessing certain files or folders. By restricting user permissions, you can reduce the impact of malware infections by preventing them from affecting other users or system components7.

---

### Question: 390

---

A technician receives a help desk ticket from a user who is unable to update a phone. The technician investigates the issue and notices the following error message: Insufficient storage space

While analyzing the phone, the technician does not discover any third-party' applications or photos. Which of the following is the best way to resolve the issue?

- A . Exchange the device for a newer one.
- B . Upgrade the onboard storage
- C . Allocate more space by removing factory applications
- D . Move factory applications to external memory.

---

**Answer: D**

---

Explanation:

The best way to resolve the issue is to move factory applications to external memory. This will free up some space on the phone's internal storage, which is required for updating the phone. To do this, you can follow these steps1:

Insert a microSD card into your phone if you don't have one already.

Go to Settings > Apps and tap on the app you want to move.

Tap on Storage and then on Change.

Select the SD card option and tap on Move.

You may need to repeat this process for multiple apps until you have enough space to update your phone. Alternatively, you can also clear the cache and data of some apps, or uninstall the apps that you don't use frequently. You can find more information on how to fix insufficient storage error on your phone in these articles234. I hope this helps.

---

### Question: 391

---

A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities is the best choice for accessing the necessary configuration to complete this goal?

- A . Security and Maintenance
- B . Network and Sharing Center
- C . Windows Defender Firewall
- D . Internet Options

---

**Answer: D**

---

Explanation:



Explore

[The correct answer is D\) Internet Options. The Internet Options utility in Windows allows you to configure various settings related to your internet connection, including the proxy server settings. To access the Internet Options utility, you can either open the Control Panel and click on Internet Options, or open any web browser and click on the Tools menu and then on Internet Options. In the Internet Options window, go to the Connections tab and click on the LAN settings button. Here, you can enable or disable the use of a proxy server, as well as enter the address and port number of the proxy server you want to use12.](#)

Security and Maintenance is a utility in Windows that allows you to view and manage the security and maintenance status of your computer, such as firewall, antivirus, backup, troubleshooting, and recovery settings. It does not have any option to configure proxy server settings.

Network and Sharing Center is a utility in Windows that allows you to view and manage your network connections, such as Wi-Fi, Ethernet, VPN, or dial-up. It also allows you to change network settings, such as network discovery, file and printer sharing, homegroup, and adapter settings. It does not have any option to configure proxy server settings.

Windows Defender Firewall is a utility in Windows that allows you to enable or disable the firewall protection for your computer, as well as configure firewall rules for inbound and outbound traffic. It does not have any option to configure proxy server settings.

---

### **Question: 392**

---

A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

- A . Factory reset
- B . System Restore
- C . In-place upgrade

#### D . Unattended installation

---

**Answer: D**

---

Explanation:



The correct answer is D) Unattended installation. An unattended installation is a way of installing Windows 10 without requiring any user input or interaction. It uses a configuration file called answer file that contains the settings and preferences for the installation, such as the product key, language, partition, and network settings. An unattended installation can be performed by using a bootable USB flash drive or DVD that contains the Windows 10 installation files and the answer file1. This is the fastest way for the technician to install Windows 10 on a newly built computer, as it automates the whole process and saves time.

A factory reset is a way of restoring a computer to its original state by deleting all the data and applications and reinstalling the operating system. A factory reset can be performed by using the recovery partition or media that came with the computer, or by using the Reset this PC option in Windows 10 settings2. A factory reset is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

A system restore is a way of undoing changes to a computer's system files and settings by using a restore point that was created earlier. A system restore can be performed by using the System Restore option in Windows 10 settings or by using the Advanced Startup Options menu3. A system restore is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system and restore points to be present.

An in-place upgrade is a way of upgrading an existing operating system to a newer version without losing any data or applications. An in-place upgrade can be performed by using the Windows 10 Media Creation Tool or by running the Setup.exe file from the Windows 10 installation medi

a. An in-place upgrade is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

---

#### **Question: 393**

---

A developer's Type 2 hypervisor is performing inadequately when compiling new source code. Which of the following components should the developer upgrade to improve the hypervisor's performance?

- A . Amount of system RAM
- B . NIC performance
- C . Storage IOPS
- D . Dedicated GPU

---

**Answer: A**

---

Explanation:

The correct answer is A) Amount of system RAM. A Type 2 hypervisor is a virtualization software that runs on top of a host operating system, which means it shares the system resources with the host OS and other applications. Therefore, increasing the amount of system RAM can improve the performance of the hypervisor and the virtual machines running on it. RAM is used to store data and instructions that are frequently accessed by the CPU, and having more RAM can reduce the need for swapping data to and from the storage device, which is slower than RAM.

NIC performance, storage IOPS, and dedicated GPU are not as relevant for improving the hypervisor's performance in this scenario. NIC performance refers to the speed and quality of the network interface card, which is used to connect the computer to a network. Storage IOPS refers to the number of input/output operations per second that can be performed by the storage device, which is a measure of its speed and efficiency. Dedicated GPU refers to a separate graphics processing unit that can handle complex graphics tasks, such as gaming or video editing. These components may affect other aspects of the computer's performance, but they are not directly related to the hypervisor's ability to compile new source code.

---

**Question: 394**

---

A company is experiencing a ODDS attack. Several internal workstations are the source of the traffic Which of the following types of infections are the workstations most likely experiencing? (Select two)

- A . Zombies
- B . Keylogger
- C . Adware
- D . Botnet
- E . Ransomware
- F . Spyware

---

**Answer: A, D**

---

Explanation:

The correct answers are A and D) Zombies and botnets are types of infections that allow malicious actors to remotely control infected computers and use them to launch distributed denial-of-service (DDoS) attacks against a target. A DDoS attack is a type of cyberattack that aims to overwhelm a server or a network with a large volume of traffic from multiple sources, causing it to slow down or crash.

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote server, often for the purpose of stealing passwords, credit card numbers, or other sensitive information.

Adware is a type of software that displays unwanted advertisements on a user's computer, often in the form of pop-ups, banners, or redirects. Adware can also collect user data and compromise the security and performance of the system.

Ransomware is a type of malware that encrypts the files or locks the screen of a user's computer and demands a ransom for their restoration. Ransomware can also threaten to delete or expose the user's data if the ransom is not paid.

Spyware is a type of software that covertly monitors and collects information about a user's online activities, such as browsing history, search queries, or personal data. Spyware can also alter the settings or functionality of the user's system without their consent.

---

### Question: 395

---

A PC is taking a long time to boot. Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

- A . Installing additional RAM
- B . Removing the applications from startup
- C . Installing a faster SSD
- D . Running the Disk Cleanup utility
- E . Defragmenting the hard drive
- F . Ending the processes in the Task Manager

---

**Answer: B, D**

---

Explanation:

The best operations to do to resolve the issue of a long boot time at a minimal expense are B. Removing the applications from startup and D. Running the Disk Cleanup utility. These are two simple and effective ways to speed up your PC's boot time without spending any money on hardware upgrades.

Removing the applications from startup means preventing unnecessary programs from launching automatically when you turn on your computer. This can reduce the load on your system resources and make the boot process faster. You can do this in Windows 10 by pressing Ctrl + Alt + Esc to open the Task Manager, and going to the Startup tab. There, you can see a list of programs that start with your computer, and their impact on the startup performance. You can disable any program that you don't need by right-clicking on it and choosing Disable12.

Running the Disk Cleanup utility means deleting temporary files, system files, and other unnecessary data that may be taking up space and slowing down your computer. This can free up some disk space and improve the performance of your system. You can do this in Windows 10 by typing disk cleanup in the search box and selecting the Disk Cleanup app. There, you can choose which files you want to delete, such as Recycle Bin, Temporary Internet Files, Thumbnails, etc. You can also click on Clean up system files to delete more files, such as Windows Update Cleanup, Previous Windows installation(s), etc34.

---

### Question: 396

---

A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

- A . Document the date and time of the change.
- B . Submit a change request form
- C . Determine the risk level of this change
- D . Request an unused IP address.

---

**Answer: B**

---

Explanation:

The correct answer is B) Submit a change request form. A change request form is a document that describes the proposed change, the reason for the change, the expected benefits and impacts, the risks and mitigation strategies, the implementation plan, and the approval process. A change request form is an essential part of change management best practices, as it helps to ensure that the change is well-planned, communicated, and authorized before it is implemented<sup>12</sup>.

A change request form should be submitted immediately before network use is authorized, because it provides the necessary information and justification for the change to the relevant stakeholders, such as the network administrator, the IT manager, and the department manager. The change request form also allows the stakeholders to review and approve or reject the change, or request more information or modifications. The change request form also serves as a record of the change history and status<sup>12</sup>.

---

### Question: 397

---

Which of the following macOS features can help a user close an application that has stopped responding?

- A . Finder
- B . Mission Control
- C . System Preferences
- D . Force Quit

---

**Answer: D**

---

Explanation:

The correct answer is D) Force Quit. Force Quit is a macOS feature that allows users to close an application that has stopped responding. To use Force Quit, users can press and hold Option (or Alt), Command, and Esc (Escape) keys together, or choose Force Quit from the Apple menu in the corner of the screen. A Force Quit window will open, where users can select the application that they want to close and click Force Quit<sup>123</sup>.

Reference and

The web search results provide information about how to force an app to quit on Mac using different methods, such as keyboard shortcuts, mouse clicks, or menu options. The results also explain what to do if the app cannot be forced to quit or if the Mac does not respond.

The first result<sup>1</sup> is from the official Apple Support website and provides detailed instructions and screenshots on how to force an app to quit on Mac using the keyboard shortcut or the Apple menu. It also explains how to force quit the Finder app and how to restart or turn off the Mac if needed.

[The second result2 is from the same website but for a different region \(UK\). It has the same content as the first result but with some minor differences in spelling and wording.](#)

[The third result4 is from a website called Lifehacker that provides tips and tricks for various topics, including technology. It compares how to close a program that is not responding on different operating systems, such as Windows, Mac, and Linux. It briefly mentions how to force quit an app on Mac using the keyboard shortcut or the mouse click.](#)

[The fourth result3 is from a website called Parallels that provides software solutions for running Windows on Mac. It focuses on how to force quit an app on Mac using the keyboard shortcut and provides a video tutorial and a screenshot on how to do it. It also suggests some alternative ways to close an app that is not responding, such as using Activity Monitor or Terminal commands.](#)

---

### **Question: 398**

---

A change advisory board authorized a setting change so a technician is permitted to implement the change. The technician successfully implemented the change. Which of the following should be done next?

- A . Document the date and time of change
- B . Document the purpose of the change.
- C . Document the risk level.
- D . Document the findings of the sandbox test,

---

### **Answer: A**

---

Explanation:

The correct answer is

A) Document the date and time of change. After implementing a change, the technician should document the date and time of change in the change log or record. This helps to track the change history, monitor the change performance, and identify any issues or incidents related to the change. Documenting the date and time of change is also a good practice for auditing and compliance purposes.

Documenting the purpose of the change (B) and the risk level are steps that should be done before implementing the change, not after. These are important information that help to justify, prioritize, and plan the change. The purpose of the change should explain why the change is needed and what benefits it will bring to the organization. The risk level should assess the potential impact and probability of the change causing any problems or disruptions to the business.

Documenting the findings of the sandbox test (D) is also a step that should be done before implementing the change, not after. A sandbox test is a way of testing the change in an isolated environment that mimics the production environment. This helps to verify that the change works as expected and does not cause any errors or conflicts with other systems or processes. The findings of the sandbox test should be documented and reviewed by the change advisory board (CAB) before approving the change for implementation.

[What is a Change Advisory Board? \(Overview, Roles, and Responsibilities\)](#)

## Best Practices in Change Management

### 10 Top change management best practices

---

#### **Question: 399**

---

A salesperson's computer is unable to print any orders on a local printer that is connected to the computer. Which of the following tools should the salesperson use to restart the print spooler?

- A . Control Panel
- B . Processes
- C . Startup
- D . Services

---

**Answer: D**

---

Explanation:

The correct answer is D) Services. The print spooler is a service that manages the print queue and sends print jobs to the printer. To restart the print spooler, the salesperson can use the Services app, which allows them to stop and start the service. Alternatively, they can also use the Task Manager or the Command Prompt to restart the print spooler.

Reference and

[The Services app is a tool that displays all the services that are running on the computer. It can be accessed by typing services.msc in the Run window or by searching for Services in the Start menu. The Services app allows users to start, stop, restart, or configure any service, including the print spooler123.](#)

[The Task Manager is a tool that shows information about the processes, applications, and services that are running on the computer. It can be accessed by pressing Ctrl + Shift + Esc or by right-clicking on the taskbar and selecting Task Manager. The Task Manager allows users to start, stop, or restart any service by going to the Services tab and right-clicking on the service name12.](#)

[The Command Prompt is a tool that allows users to execute commands and perform tasks using text input. It can be accessed by typing cmd in the Run window or by searching for Command Prompt in the Start menu. The Command Prompt allows users to start, stop, or restart any service by using the net command with the service name. For example, to restart the print spooler, users can type net stop spooler and then net start spooler1.](#)

[The Control Panel is a tool that provides access to various settings and options for the computer. It can be accessed by typing control panel in the Run window or by searching for Control Panel in the Start menu. The Control Panel does not allow users to restart the print spooler directly, but it can be used to access other tools such as Devices and Printers, Troubleshooting, or Administrative Tools2.](#)

[The Processes tab is a part of the Task Manager that shows information about the processes that are running on the computer. It can be accessed by opening the Task Manager and selecting the Processes tab. The Processes tab does not allow users to restart the print spooler directly, but it can be used to end any process that is related to printing or causing problems with the print spooler2.](#)

[The Startup tab is a part of the Task Manager that shows information about the programs that run automatically when the computer starts. It can be accessed by opening the Task Manager and selecting the Startup tab. The](#)

[Startup tab does not allow users to restart the print spooler directly, but it can be used to disable or enable any program that affects printing or interferes with the print spooler2.](#)

---

### **Question: 400**

---

Windows updates need to be performed on a department's servers. Which of the following methods should be used to connect to the server?

- A . FIP
- B . MSRA
- C . RDP
- D . VPN

---

**Answer: C**

---

Explanation:

RDP (Remote Desktop Protocol) is a protocol that allows a user to connect to and control a remote computer over a network. RDP can be used to perform Windows updates on a department's servers without physically accessing them.

---

### **Question: 401**

---

A technician discovers user input has been captured by a malicious actor. Which of the following malware types is MOST likely being used?

- A . Cryptominers
- B . Rootkit
- C . Spear phishing
- D . Keylogger

---

**Answer: D**

---

Explanation:

A keylogger is a type of malware that captures user input, such as keystrokes, mouse clicks, and clipboard data, and sends it to a malicious actor. Keyloggers can be used to steal passwords, credit card numbers, personal information, and other sensitive data.

---

### **Question: 402**

---

Which of the following would cause a corporate-owned iOS device to have an Activation Lock issue?

- A . A forgotten keychain password
- B . An employee's Apple ID used on the device
- C . An operating system that has been jailbroken
- D . An expired screen unlock code

---

**Answer: B**

---

Explanation:

Activation Lock is a feature that prevents anyone from erasing or activating an iOS device without the owner's Apple ID and password. If a corporate-owned iOS device is linked to an employee's Apple ID, it will have an Activation Lock issue when the employee leaves the company or forgets their Apple ID credentials.

---

### **Question: 403**

---

An administrator is designing and implementing a server backup system that minimizes the capacity of storage used. Which of the following is the BEST backup approach to use in conjunction with synthetic full backups?

- A . Differential
- B . Open file
- C . Archive
- D . Incremental

---

**Answer: D**

---

Explanation:

Incremental backups are backups that only include the changes made since the last backup, whether it was a full or an incremental backup. Incremental backups minimize the capacity of storage used and are often used in conjunction with synthetic full backups, which are backups that combine a full backup and subsequent incremental backups into a single backup set.

---

### **Question: 404**

---

A user reports an issue when connecting a mobile device to Bluetooth. The user states the mobile device's Bluetooth is turned on. Which of the following steps should the technician take NEXT to resolve the issue?

- A . Restart the mobile device.
- B . Turn on airplane mode.
- C . Check that the accessory is ready to pair.
- D . Clear all devices from the phone's Bluetooth settings.

---

**Answer: C**

---

Explanation:

The first step in troubleshooting a Bluetooth connection issue is to check that the accessory is ready to pair with the mobile device. Some accessories may have a button or a switch that needs to be pressed or turned on to initiate pairing mode. If the accessory is not ready to pair, the mobile device will not be able to detect it.

---

### Question: 405

---

A user's corporate laptop with proprietary work information was stolen from a coffee shop. The user logged in to the laptop with a simple password, and no other security mechanisms were in place. Which of the following would MOST likely prevent the stored data from being recovered?

- A . Biometrics
- B . Full disk encryption
- C . Enforced strong system password
- D . Two-factor authentication

---

**Answer: B**

---

Explanation:

Full disk encryption is a security mechanism that encrypts the entire data on a hard drive, making it unreadable without the correct decryption key or password. It can prevent the stored data from being recovered by unauthorized persons who steal or access the laptop. Biometrics, enforced strong system password and two-factor authentication are other security mechanisms, but they only protect the login access to the laptop, not the data on the hard drive. Verified Reference: <https://www.comptia.org/blog/what-is-full-disk-encryption>  
<https://www.comptia.org/certifications/a>

---

### Question: 406

---

A technician has been tasked with troubleshooting audiovisual issues in a conference room. The meeting presenters are unable to play a video with sound. The following error is received:

The Audio Driver is not running.

Which of the following will MOST likely resolve the issue?

- A . compmgmt.msc
- B . regedit.exe
- C . explorer.exe
- D . taskmgt.exe
- E . gpmc.msc
- F . services.msc

---

**Answer: F**

---

Explanation:

[services.msc](#) is a tool that can be used to resolve the issue of "The Audio Driver is not running" on a Windows machine. It allows a technician to view, start, stop and configure the services that run on the system, such as the Windows Audio service. [compmgmt.msc](#), [regedit.exe](#), [explorer.exe](#), [taskmgt.exe](#) and [gPMC.msc](#) are other tools that can be used for different purposes on a Windows machine, but they are not related to audio drivers or services. Verified Reference: <https://www.comptia.org/blog/what-is-services-msc> <https://www.comptia.org/certifications/a>

---

### Question: 407

---

Which of the following common security vulnerabilities can be mitigated by using input validation?

- A . Brute-force attack
- B . Cross-site scripting
- C . SQL injection
- D . Cross-site request forgery

---

**Answer: B, C**

---

Explanation:

[Cross-site scripting \(XSS\)](#) and [SQL injection](#) are common security vulnerabilities that can be mitigated by using input validation. Input validation is a technique that checks the user input for any malicious or unexpected characters or commands before processing it. XSS is an attack that injects malicious scripts into web pages to steal cookies, session tokens or other sensitive information from users or web servers. SQL injection is an attack that injects malicious SQL statements into web applications to manipulate databases, execute commands or access unauthorized data. Verified Reference: <https://www.comptia.org/blog/what-is-input-validation> <https://www.comptia.org/certifications/a>

---

### Question: 408

---

A user called the help desk to report an issue with the internet connection speed on a laptop. The technician thinks that background services may be using extra bandwidth. Which of the following tools should the technician use to investigate connections on the laptop?

- A . nslookup
- B . net use
- C . netstat
- D . net user

---

**Answer: C**

---

Explanation:

[netstat](https://www.comptia.org/blog/what-is-netstat) is a tool that can be used to investigate connections on a Windows machine. It displays information about the active TCP connections, listening ports, routing tables, network statistics, etc. [nslookup](https://www.comptia.org/certifications/a) is a tool that can be used to query DNS servers and resolve domain names to IP addresses. [net use](https://www.comptia.org/certifications/a) is a tool that can be used to connect or disconnect network drives or printers. [net user](https://www.comptia.org/certifications/a) is a tool that can be used to create or modify user accounts on a Windows machine. Verified Reference: <https://www.comptia.org/blog/what-is-netstat> <https://www.comptia.org/certifications/a>

---

### Question: 409

---

An application user received an email indicating the version of the application currently in use will no longer be sold. Users with this version of the application will no longer receive patches or updates either. Which of the following indicates a vendor no longer supports a product?

- A . AUP
- B . EULA
- C . EOL
- D . UAC

---

**Answer: C**

---

Explanation:

[EOL \(end-of-life\)](https://www.comptia.org/blog/what-is-end-of-life) is a term that indicates a vendor no longer supports a product. It means that the product will no longer be sold, updated or patched by the vendor, and that the users should migrate to a newer version or alternative product. [AUP \(acceptable use policy\)](https://www.comptia.org/certifications/a), [EULA \(end-user license agreement\)](https://www.comptia.org/certifications/a) and [UAC \(user account control\)](https://www.comptia.org/certifications/a) are not terms that indicate a vendor no longer supports a product. Verified Reference: <https://www.comptia.org/blog/what-is-end-of-life> <https://www.comptia.org/certifications/a>

---

### Question: 410

---

A systems administrator is experiencing issues connecting from a laptop to the corporate network using PKI. Which of the following tools can the systems administrator use to help remediate the issue?

- A . certmgr.msc
- B . msconfig.exe
- C . lusrmgr.msc
- D . perfmon.msc

---

**Answer: A**

---

Explanation:

[certmgr.msc](https://www.comptia.org/certifications/a) is a tool that can be used to troubleshoot issues with PKI (public key infrastructure) on a Windows machine. It allows a system administrator to view, manage and import certificates, as well as check their validity, expiration and revocation status. [msconfig.exe](https://www.comptia.org/certifications/a), [lusrmgr.msc](https://www.comptia.org/certifications/a) and [perfmon.msc](https://www.comptia.org/certifications/a) are other tools that can be used for

[different purposes on a Windows machine, but they are not related to PKI.](https://www.comptia.org/blog/what-is-certmgr-msc) Verified Reference: <https://www.comptia.org/certifications/a>

---

### Question: 411

---

A technician received a call from a user who clicked on a web advertisement. Now, every time the user moves the mouse, a pop-up display across the monitor. Which of the following procedures should the technician perform?

- A . Boot into safe mode.
- B . Perform a malware scan.
- C . Restart the machine.
- D . Reinstall the browser

---

**Answer: A, B**

---

Explanation:

[Booting into safe mode and performing a malware scan are the steps that a technician should perform when troubleshooting an issue with pop-up advertising messages on a PC. Safe mode is a diagnostic mode that starts the PC with minimal drivers and services, which can prevent the pop-up malware from running. Malware scan is a tool that can detect and remove the pop-up malware, as well as prevent further infection or damage. Investigating how the malware was installed, reinstalling the browser and restarting the machine are possible steps that can be done after booting into safe mode and performing a malware scan, depending on the situation and the results of the scan.](https://www.comptia.org/blog/how-to-boot-into-safe-mode) Verified Reference: <https://www.comptia.org/certifications/a>

---

### Question: 412

---

A user reports a virus is on a PC. The user installs additional real-time protection antivirus software, and the PC begins performing extremely slow. Which of the following steps should the technician take to resolve the issue?

- A . Uninstall one antivirus software program and install a different one.
- B . Launch Windows Update, and then download and install OS updates
- C . Activate real-time protection on both antivirus software programs
- D . Enable the quarantine feature on both antivirus software programs.
- E . Remove the user-installed antivirus software program.

---

**Answer: E**

---

Explanation:

[Removing the user-installed antivirus software program is the best way to resolve the issue of extremely slow performance caused by installing additional real-time protection antivirus software on a PC. Having more than one antivirus software program running at the same time can cause conflicts, resource consumption and performance degradation. Uninstalling one antivirus software program and installing a different one, activating real-time](#)

protection on both antivirus software programs, enabling the quarantine feature on both antivirus software programs and launching Windows Update are not effective ways to resolve the issue. Verified Reference: <https://www.comptia.org/blog/why-you-shouldnt-run-multiple-antivirus-programs-at-the-same-time> <https://www.comptia.org/certifications/a>

---

### Question: 413

---

A remote user is having issues accessing an online share. Which of the following tools would MOST likely be used to troubleshoot the Issue?

- A . Screen-sharing software
- B . Secure shell
- C . Virtual private network
- D . File transfer software

---

**Answer: A**

---

Explanation:

Screen-sharing software is a tool that allows a technician to remotely view and control a user's screen over the internet. It can be used to troubleshoot issues with accessing an online share, as well as other problems that require visual inspection or guidance. Secure shell (SSH) is a protocol that allows remote access and command execution on another device, but it does not allow screen-sharing. Virtual private network (VPN) is a protocol that creates a secure tunnel between two devices over the internet, but it does not allow remote troubleshooting. File transfer software is a tool that allows transferring files between two devices over the internet, but it does not allow screen-sharing.

Verified Reference: <https://www.comptia.org/blog/what-is-screen-sharing-software>

<https://www.comptia.org/certifications/a>

---

### Question: 414

---

The courts determined that a cybercrimes case could no longer be prosecuted due to the agency's handling of evidence. Which of the following was MOST likely violated during the investigation?

- A . Open-source software
- B . EULA
- C . Chain of custody
- D . AUP

---

**Answer: C**

---

Explanation:

Chain of custody is a process that documents how evidence is collected, handled, stored and transferred during a cybercrime investigation. It ensures that the evidence is authentic, reliable and admissible in court. If the chain of custody is violated during an investigation, it can compromise the integrity of the evidence and lead to the case being

dismissed. Open-source software, EULA (end-user license agreement) and AUP (acceptable use policy) are not related to cybercrime investigations or evidence handling. Verified Reference: <https://www.comptia.org/blog/what-is-chain-of-custody> <https://www.comptia.org/certifications/a>

---

### Question: 415

---

Which of the following operating systems is considered closed source?

- A . Ubuntu
- B . Android
- C . CentOS
- D . OSX

---

**Answer: D**

---

Explanation:

OSX (now macOS) is an operating system that is considered closed source, meaning that its source code is not publicly available or modifiable by anyone except its developers. It is owned and maintained by Apple Inc. Ubuntu, Android and CentOS are operating systems that are considered open source, meaning that their source code is publicly available and modifiable by anyone who wants to contribute or customize them.

Verified Reference: <https://www.comptia.org/blog/open-source-vs-closed-source-software> <https://www.comptia.org/certifications/a>

---

### Question: 416

---

Which of the following is used to identify potential issues with a proposed change prior to implementation?

- A . Request form
- B . Rollback plan
- C . End-user acceptance
- D . Sandbox testing

---

**Answer: D**

---

Explanation:

Sandbox testing is a method of identifying potential issues with a proposed change prior to implementation. It involves creating a simulated or isolated environment that mimics the real system and applying the change to it. This can help to verify that the change works as expected and does not cause any errors or conflicts.

Request form, rollback plan and end-user acceptance are other components of a change management process, but they do not involve identifying issues with a change.

Verified Reference: <https://www.comptia.org/blog/what-is-sandbox-testing> <https://www.comptia.org/certifications/a>

---

## **Question: 417**

---

A user is unable to access files on a work PC after opening a text document. The text document was labeled 'URGENT PLEASE READ.txt - In active folder, .txt file titled urgent please read'. Which of the following should a support technician do FIRST?

- A . Quarantine the host in the antivirus system.
- B . Run antivirus scan for malicious software.
- C . Investigate how malicious software was installed.
- D . Reimage the computer.

---

**Answer: B**

---

Explanation:

Running an antivirus scan for malicious software is the first step that a support technician should do when a user reports a virus on a PC. The antivirus scan can detect and remove the virus, as well as prevent further damage or infection. Quarantining the host, investigating how the malware was installed and reimaging the computer are possible steps that can be done after running the antivirus scan, depending on the situation and the results of the scan. Verified Reference: <https://www.comptia.org/blog/how-to-remove-a-virus>  
<https://www.comptia.org/certifications/a>

---

## **Question: 418**

---

A user has a computer with Windows 10 Home installed and purchased a Windows 10 Pro license. The user is not sure how to upgrade the OS. Which of the following should the technician do to apply this license?

- A . Copy the c:\Windows\Windows.lic file over to the machine and restart.
- B . Redeem the included activation key card for a product key.
- C . Insert a Windows USB hardware dongle and initiate activation.
- D . Activate with the digital license included with the device hardware.

---

**Answer: B**

---

Explanation:

Redeeming the included activation key card for a product key is the correct way to apply a Windows 10 Pro license to a computer that has Windows 10 Home installed. The activation key card is a physical or digital card that contains a 25-digit code that can be used to activate Windows 10 Pro online or by phone. Copying the windows.lic file, inserting a Windows USB hardware dongle and activating with the digital license are not valid methods of applying a Windows 10 Pro license. Verified Reference: <https://www.comptia.org/blog/how-to-upgrade-windows-10-home-to-pro>  
<https://www.comptia.org/certifications/a>

---

## **Question: 419**

---

Which of the following macOS utilities uses AES-128 to encrypt the startup disk?

- A . fdisk
- B . Diskpart
- C . Disk Utility
- D . FileVault

---

**Answer: D**

---

Explanation:

[FileVault is a macOS utility that uses AES-128 \(Advanced Encryption Standard\) to encrypt the startup disk of a Mac computer. It protects the data from unauthorized access if the computer is lost or stolen.](#) [fdisk and Diskpart are disk partitioning utilities for Linux and Windows, respectively.](#) [Disk Utility is another macOS utility that can perform disk management tasks, such as formatting, resizing, repairing, etc.](#) Verified Reference: <https://www.comptia.org/blog/what-is-filevault> <https://www.comptia.org/certifications/a>

---

### **Question: 420**

---

Which of the following security methods supports the majority of current Wi-Fi-capable devices without sacrificing security?

- A . WPA3
- B . MAC filleting
- C . RADIUS
- D . TACACS+

---

**Answer: A**

---

Explanation:

[WPA3 \(Wi-Fi Protected Access 3\) is a wireless security method that supports the majority of current Wi-Fi-capable devices without sacrificing security.](#) [It is backward compatible with WPA2 devices and offers enhanced encryption and authentication features.](#) [MAC filtering is another wireless security method, but it can be easily bypassed by spoofing MAC addresses.](#) [RADIUS \(Remote Authentication Dial-In User Service\) and TACACS+ \(Terminal Access Controller Access-Control System Plus\) are network authentication protocols, but they are not wireless security methods by themselves.](#) Verified Reference: <https://www.comptia.org/blog/wireless-security-standards> <https://www.comptia.org/certifications/a>

---

### **Question: 421**

---

A user reported that a laptop's screen turns off very quickly after sitting for a few moments and is also very dim when not plugged in to an outlet. Everything else seems to be functioning normally. Which of the following Windows settings should be configured?

- A . Power Plans
- B . Hibernate
- C . Sleep/Suspend
- D . Screensaver

---

**Answer: A**

---

Explanation:

Power Plans are Windows settings that allow a user to configure how a laptop's screen behaves when plugged in or running on battery power. They can adjust the screen brightness and the time before the screen turns off due to inactivity. Hibernate, Sleep/Suspend and Screensaver are other Windows settings that affect how a laptop's screen behaves, but they do not allow changing the screen brightness or turning off time. Verified Reference: <https://www.comptia.org/blog/windows-power-plans> <https://www.comptia.org/certifications/a>

---

### **Question: 422**

---

Which of The following refers to the steps to be taken if an Issue occurs during a change Implementation?

- A . Testing
- B . Rollback
- C . Risk
- D . Acceptance

---

**Answer: B**

---

Explanation:

Rollback refers to the steps to be taken if an issue occurs during a change implementation. It means restoring the system to its previous state before the change was applied, using backup data or configuration files. It can minimize the impact and downtime caused by a failed change. Testing refers to the steps to be taken before a change implementation, to verify that the change works as expected and does not cause any errors or conflicts. Risk refers to the potential negative consequences of a change implementation, such as data loss, security breach, performance degradation, etc. Acceptance refers to the steps to be taken after a change implementation, to confirm that the change meets the requirements and expectations of the stakeholders. Verified Reference: <https://www.comptia.org/blog/change-management-process> <https://www.comptia.org/certifications/a>

---

### **Question: 423**

---

A user is receiving repeated pop-up advertising messages while browsing the internet. A malware scan Is unable to locate the source of an infection. Which of the following should the technician check NEXT?

- A . Windows updates
- B . DNS settings
- C . Certificate store

## D . Browser plug-ins

---

**Answer: D**

---

Explanation:

Browser plug-ins are software components that add functionality to a web browser, such as playing videos, displaying animations, etc. However, some browser plug-ins can also be malicious or compromised and cause unwanted pop-up advertising messages while browsing the internet. A malware scan may not be able to locate the source of the infection if it is hidden in a browser plug-in. Windows updates, DNS settings and certificate store are not likely sources of pop-up advertising messages. Verified Reference: <https://www.comptia.org/blog/browser-security> <https://www.comptia.org/certifications/a>

---

## Question: 424

---

A user opened a ticket regarding a corporate-managed mobile device. The assigned technician notices the OS is several versions out of date. The user is unaware the OS version is not current because auto-update is turned on. Which of the following is MOST likely the cause of the issue?

- A . The device does not have enough free space to download the OS updates.
- B . The device needs domain administrator confirmation to update to a major release.
- C . The device is not compatible with the newest version of the OS.
- D . The device is restricted from updating due to a corporate security policy.

---

**Answer: D**

---

Explanation:

A corporate security policy can restrict a corporate-managed mobile device from updating its OS automatically, even if the auto-update feature is turned on. This can be done to prevent compatibility issues, security risks or performance problems caused by untested or unwanted updates. The device administrator can control when and how the updates are applied to the device. The device not having enough free space, needing domain administrator confirmation or being incompatible with the newest version of the OS are not likely causes of the issue, since the user would receive an error message or a notification in those cases. Verified Reference: <https://www.comptia.org/blog/mobile-device-management> <https://www.comptia.org/certifications/a>

---

## Question: 425

---

A systems administrator notices that a server on the company network has extremely high CPU utilization. Upon further inspection, the administrator sees that the server is consistently communicating with an IP address that is traced back to a company that awards digital currency for solving hash algorithms. Which of the following was MOST likely used to compromise the server?

- A . Keylogger
- B . Ransomware

- C . Boot sector virus
- D . Cryptomining malware

---

**Answer: D**

---

Explanation:

Cryptomining malware is a type of malicious program that uses the CPU resources of a compromised server to generate cryptocurrency, such as Bitcoin or Ethereum. It can cause extremely high CPU utilization and network traffic to the IP address of the cryptocurrency service. Keylogger, ransomware and boot sector virus are other types of malware, but they do not cause the same symptoms as cryptomining malware. Verified Reference: <https://www.comptia.org/blog/what-is-cryptomining> <https://www.comptia.org/certifications/a>

---

### **Question: 426**

---

A technician is selling up a newly built computer. Which of the following is the FASTEST way for the technician to install Windows 10?

- A . Factory reset
- B . System Restore
- C . In-place upgrade
- D . Unattended installation

---

**Answer: D**

---

Explanation:

An unattended installation is the fastest way to install Windows 10 on a newly built computer. It uses an answer file that contains all the configuration settings and preferences for the installation, such as language, product key, partition size, etc. It does not require any user interaction or input during the installation process. Factory reset, System Restore and in-place upgrade are not methods of installing Windows 10 on a new computer, but ways of restoring or updating an existing Windows installation. Verified Reference: <https://www.comptia.org/blog/what-is-an-unattended-installation> <https://www.comptia.org/certifications/a>

---

### **Question: 427**

---

A technician needs to establish a remote access session with a user who has a Windows workstation. The session must allow for simultaneous viewing of the workstation by both the user and technician. Which of the following remote access technologies should be used?

- A . RDP
- B . VPN
- C . SSH
- D . MSRA

Explanation:

[MSRA \(Microsoft Remote Assistance\)](https://www.comptia.org/blog/what-is-msra) is a remote access technology that allows a technician to establish a session with a user who has a Windows workstation. The session allows for simultaneous viewing of the workstation by both the user and technician, as well as remote control and file transfer capabilities. RDP (remote desktop protocol) is another remote access technology, but it does not allow simultaneous viewing by default. VPN (virtual private network) and SSH (secure shell) are protocols that create secure tunnels between two devices over the internet, but they do not allow remote access sessions. Verified Reference: <https://www.comptia.org/blog/what-is-msra> <https://www.comptia.org/certifications/a>

---

### **Question: 428**

---

A system drive is nearly full, and a technician needs to free up some space. Which of the following tools should the technician use?

- A . Disk Cleanup
- B . Resource Monitor
- C . Disk Defragment
- D . Disk Management

Explanation:

[Disk Cleanup](https://www.comptia.org/blog/how-to-use-disk-cleanup) is a tool that can free up some space on a system drive that is nearly full. It can delete temporary files, cached files, recycle bin files, old system files and other unnecessary data. [Resource Monitor](https://www.comptia.org/blog/how-to-use-disk-cleanup) is a tool that shows the network activity of each process on a Windows machine. [Disk Defragment](https://www.comptia.org/blog/how-to-use-disk-cleanup) is a tool that optimizes the performance of a hard drive by rearranging the data into contiguous blocks. [Disk Management](https://www.comptia.org/blog/how-to-use-disk-cleanup) is a tool that allows creating, formatting, resizing and deleting partitions on a hard drive. Verified Reference: <https://www.comptia.org/blog/how-to-use-disk-cleanup> <https://www.comptia.org/certifications/a>

---

### **Question: 429**

---

A company is looking for a solution that provides a backup for all data on the system while providing the lowest impact to the network. Which of the following backup types will the company MOST likely select?

- A . Off-site
- B . Synthetic
- C . Full
- D . Differential

---

**Answer: B**

---

Explanation:

A synthetic backup is a backup type that provides a backup for all data on the system while providing the lowest impact to the network. It combines a full backup with one or more incremental backups to create a single backup set, without requiring access to the original data source. Off-site is a backup location, not a backup type. Full and differential are backup types, but they have a higher impact on the network than synthetic. Verified Reference: <https://www.comptia.org/blog/what-is-a-synthetic-backup> <https://www.comptia.org/certifications/a>

---

### **Question: 430**

---

A user's permissions are limited to read on a shared network folder using NTFS security settings. Which of the following describes this type of security control?

- A . SMS
- B . MFA
- C . ACL
- D . MDM

---

**Answer: C**

---

Explanation:

[ACL \(access control list\)](#) is a security control that describes what permissions a user or group has on a shared network folder using [NTFS \(New Technology File System\)](#) security settings. It can be used to grant or deny read, write, modify, delete or execute access to files and folders. [SMS \(short message service\)](#), [MFA \(multifactor authentication\)](#), [MDM \(mobile device management\)](#) are not security controls that apply to shared network folders. Verified Reference: <https://www.comptia.org/blog/what-is-an-acl> <https://www.comptia.org/certifications/a>

---

### **Question: 431**

---

Every time a user tries to open the organization's proprietary application on an Android tablet, the application immediately closes. Other applications are operating normally. Which of the following troubleshooting actions would MOST likely resolve the issue? (Select TWO).

- A . Uninstalling the application
- B . Gaining root access to the tablet
- C . Resetting the web browser cache
- D . Deleting the application cache
- E . Clearing the application storage
- F . Disabling mobile device management

Explanation:

Uninstalling and reinstalling the application can resolve the issue of it crashing immediately on an Android tablet, as it can fix any corrupted or missing files or settings. Clearing the application storage can also resolve the issue, as it can free up space and remove any conflicting data. Gaining root access to the tablet, resetting the web browser cache, deleting the application cache and disabling mobile device management are not likely to resolve the issue, as they do not affect how the application runs. Verified Reference: <https://www.comptia.org/blog/how-to-fix-android-apps-crashing> <https://www.comptia.org/certifications/a>

---

### **Question: 432**

---

A corporation purchased new computers for a school. The computers are the same make and model and need to have the standard image loaded. Which of the following orchestration tools should a desktop administrator use for wide-scale deployment?

- A . USB drive
- B . DVD Installation media
- C . PXE boot
- D . Recovery partition

Explanation:

PXE (Preboot eXecution Environment) boot is an orchestration tool that allows a desktop administrator to deploy a standard image to multiple computers over a network. It requires a PXE server that hosts the image and a PXE client that boots from the network interface card (NIC). USB drive and DVD installation media are not orchestration tools, but manual methods of installing an image on each computer individually. Recovery partition is not an orchestration tool, but a hidden partition on the hard drive that contains an image of the factory settings. Verified Reference: <https://www.comptia.org/blog/what-is-pxe-boot> <https://www.comptia.org/certifications/a>

---

### **Question: 433**

---

A systems administrator installed the latest Windows security patch and received numerous tickets reporting slow performance the next day. Which of the following should the administrator do to resolve this issue?

- A . Rebuild user profiles.
- B . Roll back the updates.
- C . Restart the services.
- D . Perform a system file check.

---

**Answer: B**

---

Explanation:

Rolling back the updates is the best way to resolve the issue of slow performance caused by installing the latest Windows security patch. This can be done by using the System Restore feature or by uninstalling the specific update from the Control Panel. Rebuilding user profiles, restarting the services and performing a system file check are not likely to fix the issue, since they do not undo the changes made by the update. Verified Reference: <https://www.comptia.org/blog/how-to-roll-back-windows-updates> <https://www.comptia.org/certifications/a>

---

### **Question: 434**

---

A customer calls the help desk asking for instructions on how to modify desktop wallpaper. Which of the following Windows 10 settings should the technician recommend?

- A . Personalization
- B . Apps
- C . Updates
- D . Display

---

**Answer: A**

---

Explanation:

Personalization is a Windows 10 setting that allows a user to modify the desktop wallpaper, as well as other aspects of the appearance and behavior of the desktop, such as colors, themes, sounds, etc. Apps is a Windows 10 setting that allows a user to manage the installed applications and their features. Updates is a Windows 10 setting that allows a user to check for and install the latest updates for the OS and other components. Display is a Windows 10 setting that allows a user to adjust the screen resolution, brightness, orientation, etc. Verified Reference: <https://www.comptia.org/blog/windows-10-settings> <https://www.comptia.org/certifications/a>

---

### **Question: 435**

---

A technician removed a virus from a user's device. The user returned the device a week later with the same virus on it. Which of the following should the technician do to prevent future infections?

- A . Disable System Restore.
- B . Educate the end user.
- C . Install the latest OS patches.
- D . Clean the environment reinstallation.

---

**Answer: B**

---

Explanation:

Educating the end user is the best way to prevent future infections by viruses or other malware. The technician should teach the user how to avoid risky behaviors, such as opening suspicious attachments, clicking on unknown links, downloading untrusted software, etc. Disabling System Restore, installing the latest OS patches and performing a clean installation are possible ways to remove existing infections, but they do not prevent future ones. Verified Reference: <https://www.comptia.org/blog/how-to-prevent-malware> <https://www.comptia.org/certifications/a>

---

### **Question: 436**

---

A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?

- A . FAT32
- B . exFAT
- C . BitLocker
- D . EFS

---

**Answer: D**

---

Explanation:

EFS (Encrypting File System) is a feature that allows a user to encrypt a single folder or file on a Windows PC. It uses a public key encryption system to protect the data from unauthorized access. FAT32 and exFAT are file system formats that do not support encryption. BitLocker is a feature that encrypts the entire drive, not a single folder or file. Verified Reference: <https://www.comptia.org/blog/what-is-efs> <https://www.comptia.org/certifications/a>

---

### **Question: 437**

---

A user is unable to access a web-based application. A technician verifies the computer cannot access any web pages at all. The computer obtains an IP address from the DHCP server. Then, the technician verifies the user can ping localhost, the gateway, and known IP addresses on the internet and receive a response. Which of the following is the MOST likely reason for the issue?

- A . A firewall is blocking the application.
- B . The wrong VLAN was assigned.
- C . The incorrect DNS address was assigned.
- D . The browser cache needs to be cleared

---

**Answer: C**

---

Explanation:

DNS (domain name system) is a protocol that translates domain names to IP addresses. If the computer has an incorrect DNS address assigned, it will not be able to resolve the domain names of web-based applications and

access them. A firewall, a VLAN (virtual local area network) and a browser cache are not the most likely reasons for the issue, since the computer can ping known IP addresses on the internet and receive a response. Verified Reference: <https://www.comptia.org/blog/what-is-dns> <https://www.comptia.org/certifications/a>

---

### Question: 438

---

Which of the following protects a mobile device against unwanted access when it is left unattended?

- A . PIN code
- B . OS updates
- C . Antivirus software
- D . BYOD policy

---

**Answer: A**

---

Explanation:

A PIN code is a numeric password that protects a mobile device against unwanted access when it is left unattended. It requires the user to enter the correct code before unlocking the device. OS updates, antivirus software and BYOD policy are other security measures for mobile devices, but they do not prevent unauthorized access when the device is left unattended. Verified Reference: <https://www.comptia.org/blog/mobile-device-security> <https://www.comptia.org/certifications/a>

---

### Question: 439

---

A malicious file was executed automatically when a flash drive was plugged in. Which of the following features would prevent this type of incident?

- A . Disabling UAC
- B . Restricting local administrators
- C . Enabling UPnP
- D . Turning off AutoPlay

---

**Answer: D**

---

Explanation:

AutoPlay is a feature that automatically runs programs or files when a removable media device, such as a flash drive, is plugged in. This can be exploited by malware authors who place malicious files on flash drives that execute automatically when inserted into a computer. Turning off AutoPlay can prevent this type of incident by requiring the user to manually open or run files from removable media devices. Disabling UAC (user account control), restricting local administrators and enabling UPnP (universal plug and play) are not effective ways to prevent this type of incident. Verified Reference: <https://www.comptia.org/blog/autoplay-security-risk> <https://www.comptia.org/certifications/a>

---

## Question: 440

---

Which of the following Is a package management utility for PCs that are running the Linux operating system?

- A . chmod
- B . yum
- C . man
- D . grep

---

**Answer: B**

---

Explanation:

[yum \(Yellowdog Updater Modified\)](#) is a package management utility for PCs that are running the Linux operating system. It can be used to install, update and remove software packages from repositories. [chmod \(change mode\)](#) is a command that changes the permissions of files and directories in Linux. [man \(manual\)](#) is a command that displays the documentation of other commands in Linux. [grep \(global regular expression print\)](#) is a command that searches for patterns in text files in Linux. Verified Reference: <https://www.comptia.org/blog/linux-package-management> <https://www.comptia.org/certifications/a>

---

## Question: 441

---

Which of the following wireless security features can be enabled lo allow a user to use login credentials to attach lo available corporate SSIDs?

- A . TACACS+
- B . Kerberos
- C . Preshared key
- D . WPA2/AES

---

**Answer: D**

---

Explanation:

[WPA2/AES \(Wi-Fi Protected Access 2/Advanced Encryption Standard\)](#) is a wireless security standard that supports enterprise mode, which allows a user to use login credentials (username and password) to authenticate to available corporate SSIDs (service set identifiers). [TACACS+ \(Terminal Access Controller Access-Control System Plus\)](#) and [Kerberos](#) are network authentication protocols, but they are not wireless security features. Preshared key is another wireless security feature, but it does not use login credentials. Verified Reference: <https://www.comptia.org/blog/wireless-security-standards> <https://www.comptia.org/certifications/a>

---

## Question: 442

---

A user attempts to install additional software and receives a UAC prompt. Which of the following is the BEST way to resolve this issue?

- A . Add a user account to the local administrator's group.
- B . Configure Windows Defender Firewall to allow access to all networks.
- C . Create a Microsoft account.
- D . Disable the guest account.

---

**Answer: A**

---

Explanation:

A user account that belongs to the local administrator's group has the permission to install software on a Windows machine. If a user receives a UAC (user account control) prompt when trying to install software, it means the user does not have enough privileges and needs to enter an administrator's password or switch to an administrator's account. Adding the user account to the local administrator's group can resolve this issue. Configuring Windows Defender Firewall, creating a Microsoft account and disabling the guest account are not related to this issue. Verified Reference: <https://www.comptia.org/blog/user-account-control> <https://www.comptia.org/certifications/a>

---

### **Question: 443**

---

Which of the following physical security controls can prevent laptops from being stolen?

- A . Encryption
- B . LoJack
- C . Multifactor authentication
- D . Equipment lock
- E . Bollards

---

**Answer: D**

---

Explanation:

An equipment lock is a physical security device that attaches a laptop to a fixed object, such as a desk or a table, with a cable and a lock. This can prevent the laptop from being stolen by unauthorized persons. Encryption, LoJack, multifactor authentication and bollards are other security measures, but they do not physically prevent theft. Verified Reference: <https://www.comptia.org/blog/physical-security> <https://www.comptia.org/certifications/a>

---

### **Question: 444**

---

An Internet cafe has several computers available for public use. Recently, users have reported the computers are much slower than they were the previous week. A technician finds the CPU is at 100% utilization, and antivirus scans report no current infection. Which of the following is MOST likely causing the issue?

- A . Spyware is redirecting browser searches.

- B . A cryptominer is verifying transactions.
- C . Files were damaged from a cleaned virus infection.
- D . A keylogger is capturing user passwords.

---

**Answer: B**

---

Explanation:

A cryptominer is a malicious program that uses the CPU resources of a computer to generate cryptocurrency, such as Bitcoin or Ethereum. This can cause the CPU to run at 100% utilization and slow down the system. Spyware, virus and keylogger are other types of malware, but they do not necessarily cause high CPU usage. Verified Reference: <https://www.comptia.org/blog/what-is-cryptomining> <https://www.comptia.org/certifications/a>

---

### **Question: 445**

---

A user's iPhone was permanently locked after several failed login attempts. Which of the following will restore access to the device?

- A . Fingerprint and pattern
- B . Facial recognition and PIN code
- C . Primary account and password
- D . Secondary account and recovery code

---

**Answer: D**

---

Explanation:

A secondary account and recovery code are used to reset the primary account and password on an iPhone after it has been locked due to failed login attempts. Fingerprint, pattern, facial recognition and PIN code are biometric or numeric methods that can be used to unlock an iPhone, but they are not helpful if the device has been permanently locked. Verified Reference: <https://support.apple.com/en-us/HT204306> <https://www.comptia.org/certifications/a>

---

### **Question: 446**

---

A developer receives the following error while trying to install virtualization software on a workstation:

VTx not supported by system

Which of the following upgrades will MOST likely fix the issue?

- A . Processor
- B . Hard drive
- C . Memory
- D . Video card

---

**Answer: A**

---

Explanation:

The processor is the component that determines if the system supports virtualization technology (VTx), which is required for running virtualization software. The hard drive, memory and video card are not directly related to VTx support, although they may affect the performance of the virtual machines. Verified Reference: <https://www.comptia.org/blog/what-is-virtualization> <https://www.comptia.org/certifications/a>

---

### **Question: 447**

---

A systems administrator is monitoring an unusual amount of network traffic from a kiosk machine and needs to investigate to determine the source of the traffic. Which of the following tools can the administrator use to view which processes on the kiosk machine are connecting to the internet?

- A . Resource Monitor
- B . Performance Monitor
- C . Command Prompt
- D . System Information

---

**Answer: A**

---

Explanation:

Resource Monitor is a tool that shows the network activity of each process on a Windows machine, including the TCP connections and the sent and received bytes. Performance Monitor is a tool that shows the performance metrics of the system, such as CPU, memory, disk and network usage. Command Prompt is a tool that allows running commands and scripts on a Windows machine. System Information is a tool that shows the hardware and software configuration of a Windows machine. Verified Reference: <https://www.comptia.org/blog/how-to-use-resource-monitor> <https://www.comptia.org/certifications/a>

---

### **Question: 448**

---

A technician is creating a tunnel that hides IP addresses and secures all network traffic. Which of the following protocols is capable of enduring enhanced security?

- A . DNS
- B . IPS
- C . VPN
- D . SSH

---

**Answer: C**

---

Explanation:

A VPN (virtual private network) is a protocol that creates a secure tunnel between two devices over the internet, hiding their IP addresses and encrypting their traffic. DNS (domain name system) is a protocol that translates domain names to IP addresses. IPS (intrusion prevention system) is a device that monitors and blocks malicious network traffic. SSH (secure shell) is a protocol that allows remote access and command execution on another device. Verified Reference: <https://www.comptia.org/blog/what-is-a-vpn> <https://www.comptia.org/certifications/a>

---

### Question: 449

---

A small-office customer needs three PCs to be configured in a network with no server. Which of the following network types is the customer's BEST choice for this environment?

- A . Workgroup network
- B . Public network
- C . Wide area network
- D . Domain network

---

**Answer: A**

---

Explanation:

A workgroup network is a peer-to-peer network where each PC can share files and resources with other PCs without a central server. A public network is a network that is accessible to anyone on the internet. A wide area network is a network that spans a large geographic area, such as a country or a continent. A domain network is a network where a server controls the access and security of the PCs. Verified Reference: <https://www.comptia.org/blog/network-types> <https://www.comptia.org/certifications/a>

---

### Question: 450

---

A company is retiring old workstations and needs a certificate of destruction for all hard drives. Which of the following would be BEST to perform on the hard drives to ensure the data is unrecoverable? (Select TWO).

- A . Standard formatting
- B . Drilling
- C . Erasing
- D . Recycling
- E . Incinerating
- F . Low-level formatting

---

**Answer: B, E**

---

Explanation:

Drilling and incinerating are physical destruction methods that make the data on hard drives unrecoverable. Standard formatting, erasing and low-level formatting are logical methods that can be reversed with data recovery tools.  
Recycling is not a destruction method at all. Verified Reference: <https://www.comptia.org/blog/what-is-a-certificate-of-destruction> <https://www.comptia.org/certifications/a>

Topic 4, Exam Pool D

---

### **Question: 451**

---

A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

- A . Delete the application's cache.
- B . Check for application updates.
- C . Roll back the OS update.
- D . Uninstall and reinstall the application.

---

**Answer: B**

---

Explanation:

Checking for application updates is the first troubleshooting step that the user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue. Deleting the application's cache, rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates. Reference: :  
<https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives> :  
<https://www.lifewire.com/how-to-update-apps-on-android-4173855>

---

### **Question: 452**

---

A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

- A . Trojan
- B . Rootkit
- C . Cryptominer
- D . Keylogger

---

**Answer: D**

---

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker. A keylogger can be used to steal passwords, credit card numbers, personal information, and other sensitive data. A

keylogger can be delivered through a USB drive that contains a malicious executable file, such as grabber.exe, and an output file that stores the captured keystrokes, such as output.txt. The other options are not likely to use this method of attack. Reference: : <https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives> : <https://www.kaspersky.com/resource-center/definitions/keylogger>

---

### Question: 453

---

A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?

- A . System
- B . Network and Sharing Center
- C . User Accounts
- D . Security and Maintenance

---

Answer: C

---

Explanation:

[User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a local computer. The technician can use this utility to add a user to the local administrators group, which grants the user local administrative access to the workstation. The other options are not relevant for this task.](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/manage-user-accounts-and-groups) Reference: : <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/manage-user-accounts-and-groups>

---

### Question: 454

---

Which of the following is MOST likely used to run .vbs files on Windows devices?

- A . winmgmt.exe
- B . powershell.exe
- C . cscript.exe
- D . explorer.exe

---

Answer: C

---

Explanation:

[A .vbs file is a Virtual Basic script written in the VBScript scripting language. It contains code that can be executed within Windows via the Windows-based script host \(Wscript.exe\), to perform certain admin and processing functions1. Cscript.exe is a command-line version of the Windows Script Host that provides command-line options for setting script properties. Therefore, cscript.exe is most likely used to run .vbs files on Windows devices.](https://fileinfo.com/extension/vbs) Reference:1: <https://fileinfo.com/extension/vbs> : <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cscript>

---

## **Question: 455**

---

A customer called the help desk to report that a machine that was recently updated is no longer working. The support technician checks the latest logs to see what updates were deployed, but nothing was deployed in more than three weeks. Which of the following should the support technician do to BEST resolve the situation?

- A . Offer to wipe and reset the device for the customer.
- B . Advise that the help desk will investigate and follow up at a later date.
- C . Put the customer on hold and escalate the call to a manager.
- D . Use open-ended questions to further diagnose the issue.

---

**Answer: D**

---

Explanation:

Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution. Some examples of open-ended questions are:

What exactly is not working on your machine?

When did you notice the problem?

How often does the problem occur?

What were you doing when the problem happened?

What have you tried to fix the problem?

Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

---

## **Question: 456**

---

A technician needs to transfer a file to a user's workstation. Which of the following would BEST accomplish this task utilizing the workstation's built-in protocols?

- A . VPN
- B . SMB
- C . RMM
- D . MSRA

---

**Answer: B**

---

Explanation:

SMB stands for Server Message Block, which is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. SMB is a built-in protocol in Windows operating systems and can be used to transfer files between computers over a network. The technician can use SMB to access a file share on the user's workstation and copy the file to or from it. VPN stands for virtual private network, which is a technology that creates a secure and encrypted connection over a public network. VPN is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. RMM stands for remote monitoring and management, which is a type of software solution that allows remote management and monitoring of devices and networks. RMM is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. MSRA stands for Microsoft Remote Assistance, which is a feature that allows a user to invite another user to view or control their computer remotely. MSRA is not a protocol, but an application that uses Remote Desktop Protocol (RDP) to establish a connection. MSRA does not directly transfer files between computers.

<https://www.pc当地.com/picks/the-best-desktop-workstations>

---

**Question: 457**

---

An IT security team is implementing a new Group Policy that will return a computer to the login after three minutes. Which of the following BEST describes the change in policy?

- A . Login times
- B . Screen lock
- C . User permission
- D . Login lockout attempts

---

**Answer: B**

---

Explanation:

Screen lock is a feature that returns a computer to the login screen after a period of inactivity, requiring the user to enter their credentials to resume their session. Screen lock can be configured using Group Policy settings, such as Screen saver timeout and Interactive logon: Machine inactivity limit. Screen lock can help prevent unauthorized access to a computer when the user is away from their desk. Login times are not a feature that returns a computer to the login screen, but a measure of how long it takes for a user to log in to a system. User permission is not a feature that returns a computer to the login screen, but a set of rights and privileges that determine what a user can do on a system. Login lockout attempts are not a feature that returns a computer to the login screen, but a security policy that locks out a user account after a number of failed login attempts. <https://woshub.com/windows-lock-screen-after-idle-via-gpo/>

---

**Question: 458**

---

A technician is working on a way to register all employee badges and associated computer IDs. Which of the following options should the technician use in order to achieve this objective?

- A . Database system
- B . Software management
- C . Active Directory description
- D . Infrastructure as a Service

---

**Answer: A**

---

Explanation:

A database system is a software application that allows storing, organizing, and managing data in a structured way. A database system can be used to register all employee badges and associated computer IDs by creating a table or a record for each employee that contains their badge number, computer ID, name, and other relevant information. A database system can also facilitate searching, updating, and deleting data as needed. Software management is a general term that refers to the process of planning, developing, testing, deploying, and maintaining software applications. It does not directly address the issue of registering employee badges and computer IDs. Active Directory description is a field in Active Directory that can be used to store additional information about an object, such as a user or a computer. It is not a software application that can be used to register employee badges and computer IDs by itself. Infrastructure as a Service (IaaS) is a cloud computing model that provides servers, storage, networking, and software over the internet. It does not directly address the issue of registering employee badges and computer IDs either.

<https://www.idcreator.com/>

<https://www.alphacard.com/photo-id-systems/card-type/employee-badges>

---

### **Question: 459**

---

A company implemented a BYOD policy and would like to reduce data disclosure caused by malware that may infect these devices. Which of the following should the company deploy to address these concerns?

- A . UAC
- B . MDM
- C . LDAP
- D . SSO

---

**Answer: B**

---

Explanation:

MDM stands for mobile device management, which is a type of software solution that allows remote management and security of mobile devices. MDM can help a company reduce data disclosure caused by malware that may infect these devices by enforcing security policies, such as encryption, password protection, antivirus software, and remote wipe. MDM can also monitor and control the access of personal devices to corporate data and networks. UAC stands for user account control, which is a feature of Windows that prompts users for permission or an administrator password before making changes that affect the system. UAC may not be effective in preventing malware infection or

data disclosure on personal devices. LDAP stands for lightweight directory access protocol, which is a protocol for accessing and managing information stored in a directory service, such as user names and passwords. LDAP does not directly address the issue of malware infection or data disclosure on personal devices. SSO stands for single sign-on, which is a feature that allows users to access multiple applications or services with one set of credentials. SSO may not prevent malware infection or data disclosure on personal devices, and may even increase the risk if the credentials are compromised.

<https://www.nist.gov/news-events/news/2021/03/mobile-device-security-bring-your-own-device-byod-draft-sp-1800-22>

---

### Question: 460

---

Which of the following default system tools can be used in macOS to allow the technician to view the screen simultaneously with the user?

- A . Remote Assistance
- B . Remote Desktop Protocol
- C . Screen Sharing
- D . Virtual Network Computing

---

**Answer: C**

---

Explanation:

Screen Sharing is the default system tool that can be used in macOS to allow the technician to view the screen simultaneously with the user. Screen Sharing is a built-in app that lets users share their Mac screen with another Mac on the network. The user can enable screen sharing in the System Preferences > Sharing pane, and then allow other users to request or enter a password to access their screen<sup>1</sup>. The technician can launch the Screen Sharing app from the Spotlight search or the Finder sidebar, and then enter the user's name, address, or Apple ID to connect to their screen<sup>2</sup>. Remote Assistance is a Windows feature that allows users to invite someone to help them with a problem on their PC<sup>3</sup>. Remote Desktop Protocol (RDP) is a protocol that allows users to connect to a remote computer over a network<sup>4</sup>. Virtual Network Computing (VNC) is a technology that allows users to share their screen with other devices using a VNC viewer app<sup>1</sup>. These are not default system tools in macOS, although they can be used with third-party software or settings.

---

### Question: 461

---

A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?

- A . Open Settings, select Accounts, select Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper.
- B . Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper.
- C . Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper.

D . Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.

---

**Answer: B**

---

Explanation:

[The user can change the wallpaper using a Windows 10 Settings tool by following these steps12:](#)

Open Settings by pressing the Windows key and typing Settings, or by clicking the gear icon in the Start menu.

Select Personalization from the left navigation menu.

On the right side of the window, click Background.

In the Background settings, click the drop-down menu and select Picture as the background type.

Click Browse and then locate and open the image the user wants to use as the wallpaper.

The other options are incorrect because they do not lead to the Background settings or they do not allow the user to browse for an image. Accounts, System, and Apps are not related to personalization settings. Your info, Display, and Apps & features are not related to wallpaper settings.

---

### **Question: 462**

---

A macOS user is installing a new application. Which of the following system directories is the software MOST likely to install by default?

- A . /etc/services
- B . /Applications
- C . /usr/bin
- D . C:\Program Files

---

**Answer: B**

---

Explanation:

[The software is most likely to install by default in the /Applications directory, which is the standard location for macOS applications. This directory can be accessed from the Finder sidebar or by choosing Go > Applications from the menu bar. The /Applications directory contains all the applications that are available to all users on the system1. Some applications might also offer the option to install in the ~/Applications directory, which is a personal applications folder for a single user2. The /etc/services directory is a system configuration file that maps service names to port numbers and protocols3. The /usr/bin directory is a system directory that contains executable binaries for various commands and utilities4. The C:\Program Files directory is a Windows directory that does not exist on macOS.](#)

---

### **Question: 463**

---

An employee calls the help desk regarding an issue with a laptop PC. After a Windows update, the user can no longer use certain locally attached devices, and a reboot has not fixed the issue. Which of the following should the technician perform to fix the issue?

- A . Disable the Windows Update service.
- B . Check for updates.
- C . Restore hidden updates.
- D . Rollback updates.

---

**Answer: D**

---

Explanation:

The technician should perform a rollback of the Windows update that caused the issue with the locally attached devices. A rollback is a process of uninstalling an update and restoring the previous version of the system. This can help to fix any compatibility or performance issues caused by the update1. To rollback an update, the technician can use the Settings app, the Control Panel, or the System Restore feature. The technician should also check for any device driver updates that might be needed after rolling back the update. Disabling the Windows Update service is not a good practice, as it can prevent the system from receiving important security and feature updates. Checking for updates might not fix the issue, as the update that caused the issue might still be installed. Restoring hidden updates is not relevant, as it only applies to updates that have been hidden by the user to prevent them from being installed2.

---

### **Question: 464**

---

A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?

- A . The system is missing updates.
- B . The systems utilizing a 32-bit OS.
- C . The system's memory is failing.
- D . The system requires BIOS updates.

---

**Answer: B**

---

Explanation:

The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use1. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory2. The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.

---

### **Question: 465**

---

A technician is in the process of installing a new hard drive on a server but is called away to another task. The drive has been unpackaged and left on a desk. Which of the following should the technician perform before leaving?

- A . Ask coworkers to make sure no one touches the hard drive.
- B . Leave the hard drive on the table; it will be okay while the other task is completed.
- C . Place the hard drive in an antistatic bag and secure the area containing the hard drive.
- D . Connect an electrostatic discharge strap to the drive.

---

**Answer: C**

---

Explanation:

The technician should place the hard drive in an antistatic bag and secure the area containing the hard drive before leaving. This will protect the hard drive from electrostatic discharge (ESD), dust, moisture, and physical damage. Asking coworkers to make sure no one touches the hard drive is not a reliable or secure way to prevent damage. Leaving the hard drive on the table exposes it to ESD and other environmental hazards. Connecting an electrostatic discharge strap to the drive is not enough to protect it from dust, moisture, and physical damage.

---

### **Question: 466**

---

A change advisory board authorized a setting change so a technician is permitted to implement the change. The technician successfully implemented the change. Which of the following should be done NEXT?

- A . Document the date and time of change.
- B . Document the purpose of the change.
- C . Document the risk level.
- D . Document findings of the sandbox test.

---

**Answer: A**

---

Explanation:

After implementing a change authorized by the change advisory board (CAB), the technician should document the date and time of change as part of the post-implementation review. This helps to track the change history, verify the success of the change, and identify any issues or incidents caused by the change.1. Documenting the purpose of the change, the risk level, and the findings of the sandbox test are all part of the pre-implementation activities that should be done before submitting the change request to the CAB.

---

### **Question: 467**

---

A systems administrator is creating periodic backups of a folder on a Microsoft Windows machine. The source data is very dynamic, and files are either added or deleted regularly. Which of the following utilities can be used to 'mirror' the source data for the backup?

- A . copy
- B . xcopy
- C . robocopy
- D . Copy-Item

---

**Answer: C**

---

Explanation:

[Robocopy is a command-line utility that can be used to mirror the source data for the backup. It can copy files and folders with various options, such as copying only changed files, preserving attributes and permissions, and retrying failed copies. Robocopy is more powerful and flexible than copy or xcopy, which are simpler commands that can only copy files and folders without mirroring or other advanced features.](#) [Copy-Item is a PowerShell cmdlet that can also copy files and folders, but it is not a native Windows utility and it requires PowerShell to run1.](#)

---

### **Question: 468**

---

#### SIMULATION

A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program.

However, other employees can successfully use the Testing program.

#### INSTRUCTIONS

Review the information in each tab to verify the results of the deployment and resolve any issues discovered by selecting the:

Index number of the Event Viewer issue

First command to resolve the issue

Second command to resolve the issue

BSOD

A problem has been detected and system has been shutdown to prevent damage to your computer.

DRIVER\_IRQL\_NOT\_LESS\_OR\_EQUAL

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any system updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

\*\*\* STOP: 0x000000D1 (0x0000000R, 0x00000007, 0x00000000, 0xG74H2574)

\*\*\* strl.sys - Address G74H2574 base at G74H0000, DateStamp 4eh2534df

Beginning dump of physical memory

Physical memory dump complete.

Contact your system administrator or technical support group for further assistance.

Commands:

The screenshot shows a user interface for running commands on a system that has experienced a BSOD. At the top, there is a navigation bar with tabs: 'BSOD' (selected), 'Commands' (highlighted in blue), 'Event Viewer', 'System Error', and 'Show Question'. Below the navigation bar is a text input field containing the placeholder 'Select a command'. A dropdown menu is open, listing several PowerShell commands: 'Get-WmiObject win32\_computerSystem', 'Get-WmiObject win32\_logicaldisk', 'ls msvc\*', 'ls', and 'tasklist | sort'. The background of the interface is dark, and the text is white or light-colored.

Event Viewer:

BSOD

Commands

Event Viewer

System Error

Show Question

Index	Time	EntryType	Source	InstanceID	Message
2191	Mar 03 10:35	Information	Service Control M...	1073748860	The Multimedia Class Schedul
2190	Mar 03 10:35	Error	Application Error	100	Application has encountered
2189	Mar 03 10:29	Information	Service Control M...	1073748860	The TCP/IP NetBIOS Helper se
2188	Mar 03 10:29	Information	Service Control M...	1073748860	The Multimedia Class Schedul
2187	Mar 03 10:29	Information	MsInstaller	1033	Error Code 0: Windows Instal
2186	Mar 03 10:29	Warning	DistributedCOM	10016	The application-specific per
2185	Mar 03 10:29	Information	MEIx64	1074200578	Intel(R) Management Engine I
2184	Mar 03 10:29	Information	MEIx64	1074200578	Intel(R) Management Engine I

System Error:

BSOD

Commands

Event Viewer

System Error

Show Question



The program can't start because MSVCP100.dll is missing from your computer. Try reinstalling the program to fix this problem.

**Select Event Viewer Issue**

2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191

**Event Viewer Issue****Select Event Viewer Issue****Select Resolution**

```
reg /s "msvcp100.reg"
Get-WmiObject win32_computerSystem
setx path "C:\Windows\System32"
Get-EventLog -LogName System -Newest 8
regsvr32 msACP100.dll
robocopy "\\User-PC02\C$\Windows\System32" "C:\Program Files (x86)\Testing" "msACP100.dll"
Get-WmiObject win32_logicalDisk
shutdown -s -f -t 0
gpupdate /force
copy "C:\Program Files\Testing\msACP100.dll" "\\User-PC02\C$\Windows\System32" /v /y
ls msvc*
tasklist | sort
```

**Event Viewer Issue****1st CLI Resolution****Select Resolution**

A . see the answer below in explanation

---

**Answer: A**

---

Explanation:

**Event Viewer Issue**

2187

**1st CLI Resolution**

```
copy "C:\Program Files\Testing\msACP100.dll" "\\User-PC02\C$\Windows\System32" /v /y
```

The user is experiencing a system error that prevents them from using the Testing program. The error message indicates that the file MSVCP100.dll is missing from the computer. This file is part of the Microsoft Visual C++ 2010 Redistributable Package, which is required by some applications to run properly. The error may have occurred due to a corrupted or incomplete software deployment.

To resolve this issue, the user needs to restore the missing file and register it in the system. One possible way to do this is to copy the file from another computer that has the Testing program installed and working, and then use the regsvr32 command to register it. The steps are as follows:

On another computer (User-PC02) that has the Testing program installed and working, locate the file MSVCP100.dll in the folder C:\Program Files\Testing.

Share the folder C:\Windows\System32 on User-PC02 by right-clicking on it, selecting Properties, then Sharing, then Advanced Sharing, then checking Share this folder, then clicking OK.

On the user's computer (User-PC01), open a command prompt as an administrator by clicking Start, typing cmd, right-clicking on Command Prompt, and selecting Run as administrator.

In the command prompt, type the following command to copy the file MSVCP100.dll from User-PC02 to User-PC01:  
copy 'C:\Program Files\Testing\msvcp100.dll' '\\User-PC02\C\$\Windows\System32'

After the file is copied, type the following command to register it in the system:  
regsvr32 msvcp100.dll

Restart the user's computer and try to run the Testing program again.

Therefore, based on the instructions given by the user, the correct answers are:

Select Event Viewer Issue:2187

Select First Command:copy 'C:\Program Files\Testing\msvcp100.dll' '\\User-PC02\C\$\Windows\System32'

Select Second Command:regsvr32 msvcp100.dll

---

### Question: 469

---

Which of the following is used as a password manager in the macOS?

- A . Terminal
- B . FileVault
- C . Privacy
- D . Keychain

---

**Answer: D**

---

Explanation:

Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites1. You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them1. Keychain can also sync your passwords and other secure information across your devices using iCloud Keychain1. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords.

---

### Question: 470

---

A SOHO client is having trouble navigating to a corporate website. Which of the following should a technician do to allow access?

- A . Adjust the content filtering.
- B . Unmap port forwarding.
- C . Disable unused ports.
- D . Reduce the encryption strength

---

**Answer: A**

---

Explanation:

Content filtering is a process that manages or screens access to specific emails or webpages based on their content categories1.Content filtering can be used by organizations to control content access through their firewalls and enforce corporate policies around information system management2. A SOHO client may have content filtering enabled on their network and may need to adjust it to allow access to a corporate website that is blocked by default. The client can use a software program, a hardware device, or a subscription service to configure the content filtering settings and whitelist the desired website2.

---

### Question: 471

---

A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

- A . Trojan
- B . Rootkit
- C . Cryptominer
- D . Keylogger

---

Answer: D

---

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker1. The attacker can use the captured information to steal passwords, credit card numbers, or other sensitive dat

a.A keylogger can be installed on a computer by attaching a small USB drive that contains a malicious executable file, such as grabber.exe2. The output.txt file may contain the recorded keystrokes. The user should remove the USB drive and scan the computer for malware.

---

### Question: 472

---

A user receives an error message from an online banking site that states the following:

Your connection is not private. Authority invalid.

Which of the following actions should the user take NEXT?

- A . Proceed to the site.
- B . Use a different browser.
- C . Report the error to the bank.
- D . Reinstall the browser.

---

Answer: C

---

## Explanation:

The error message "Your connection is not private. Authority invalid." means that the web browser cannot verify the identity or security of the website's SSL certificate. This could indicate that the website has been compromised, has a configuration error, or has an expired or invalid certificate. The user should not proceed to the site or use a different browser, as this could expose their sensitive information to potential attackers. The user should also not reinstall the browser, as this is unlikely to fix the error and could cause data loss. The best action for the user to take is to report the error to the bank and wait for them to resolve it.

---

### Question: 473

---

A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?

- A . System
- B . Network and Sharing Center
- C . User Accounts
- D . Security and Maintenance

---

**Answer: C**

---

## Explanation:

User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a workstation1. The technician can use User Accounts to grant local administrative access to a user by adding the user to the Administrators group1. The Administrators group has full control over the workstation and can perform tasks such as installing software, changing system settings, and accessing all files.

---

### Question: 474

---

A user receives the following error while attempting to boot a computer.

BOOTMGR is missing

press Ctrl+Alt+Del to restart

Which of the following should a desktop engineer attempt FIRST to address this issue?

- A . Repair Windows.
- B . Partition the hard disk.
- C . Reimage the workstation.
- D . Roll back the updates.

---

**Answer: A**

---

Explanation:

The error "BOOTMGR is missing" indicates that the boot sector is damaged or missing1.The boot sector is a part of the hard disk that contains the code and information needed to start Windows1.To fix this error, one of the possible methods is to run Startup Repair from Windows Recovery Environment (WinRE)1.Startup Repair is a tool that can automatically diagnose and repair problems with the boot process2.

---

### Question: 475

---

A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

- A . Remote wipe
- B . Firewall
- C . Device encryption
- D . Remote backup
- E . Antivirus
- F . Global Positioning System

---

**Answer: A, C**

---

Explanation:

Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner1.It is used to protect data from being compromised if the device is lost, stolen, or changed hands1.Device encryption is a feature that helps protect the data on a device by making it unreadable to unauthorized users2.It requires a key or a password to access the data2. Both features can help mitigate the risk of losing company trade secrets if a corporate phone is stolen.

---

### Question: 476

---

A systems administrator is creating a new document with a list of the websites that users are allowed to access. Which of the following types of documents is the administrator MOST likely creating?

- A . Access control list
- B . Acceptable use policy
- C . Incident report
- D . Standard operating procedure

---

**Answer: A**

---

Explanation:

An access control list (ACL) is a list of permissions associated with a system resource (object), such as a website. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects<sup>1</sup>. A systems administrator can create an ACL to define the list of websites that users are allowed to access.

---

### Question: 477

---

A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

- A . Password-protected Wi-Fi
- B . Port forwarding
- C . Virtual private network
- D . Perimeter network

---

Answer: C

---

Explanation:

A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN allows remote employees to access the corporate intranet as if they were physically connected to the local network<sup>3</sup>. Password-protected Wi-Fi is a security measure for wireless networks that does not provide access to the corporate intranet. Port forwarding is a technique that allows external devices to access services on a private network through a router, but does not provide access to the corporate intranet. A perimeter network is a network segment that lies between an internal network and an external network, such as the internet, and provides an additional layer of security, but does not provide access to the corporate intranet.

---

### Question: 478

---

Which of the following often uses an SMS or third-party application as a secondary method to access a system?

- A . MFA
- B . WPA2
- C . AES
- D . RADIUS

---

Answer: A

---

Explanation:

MFA (Multi-Factor Authentication) is a security measure that often uses an SMS or third-party application as a secondary method to access a system. MFA requires the user to provide two or more pieces of evidence to prove their identity, such as something they know (e.g., password), something they have (e.g., phone), or something they are (e.g., fingerprint)<sup>2</sup>. WPA2 (Wi-Fi Protected Access 2) is a security protocol for wireless networks that does not use SMS or third-party applications. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that does

not use SMS or third-party applications. RADIUS (Remote Authentication Dial-In User Service) is a network protocol that provides centralized authentication and authorization for remote access clients, but does not use SMS or third-party applications.

---

### Question: 479

---

A technician needs to access a Windows 10 desktop on the network in a SOHO using RDP. Although the connection is unsuccessful, the technician is able to ping the computer successfully. Which of the following is MOST likely preventing the connection?

- A . The Windows 10 desktop has Windows 10 Home installed.
- B . The Windows 10 desktop does not have DHCP configured.
- C . The Windows 10 desktop is connected via Wi-Fi.
- D . The Windows 10 desktop is hibernating.

---

**Answer: A**

---

Explanation:

The Windows 10 desktop has Windows 10 Home installed, which does not support RDP (Remote Desktop Protocol) as a host. Only Windows 10 Pro, Enterprise, and Education editions can act as RDP hosts and allow remote access to their desktops<sup>1</sup>. The Windows 10 desktop does not have DHCP configured, is connected via Wi-Fi, or is hibernating are not likely to prevent the RDP connection if the technician is able to ping the computer successfully.

---

### Question: 480

---

A computer on a corporate network has a malware infection. Which of the following would be the BEST method for returning the computer to service?

- A . Scanning the system with a Linux live disc, flashing the BIOS, and then returning the computer to service
- B . Flashing the BIOS, reformatting the drive, and then reinstalling the OS
- C . Degaussing the hard drive, flashing the BIOS, and then reinstalling the OS
- D . Reinstalling the OS, flashing the BIOS, and then scanning with on-premises antivirus

---

**Answer: B**

---

Explanation:

Flashing the BIOS, reformatting the drive, and then reinstalling the OS is the best method for returning a computer with a malware infection to service. Flashing the BIOS updates the firmware of the motherboard and can remove any malware that may have infected it. Reformatting the drive erases all data on it and can remove any malware that may have infected it. Reinstalling the OS restores the system files and settings to their original state and can remove any malware that may have modified them. Scanning the system with a Linux live disc may not detect or remove all malware infections. Degaussing the hard drive is an extreme method of destroying data that may damage the drive

beyond repair. Reinstalling the OS before flashing the BIOS or scanning with antivirus may not remove malware infections that persist in the BIOS or other files.

---

### Question: 481

---

A technician receives a call from a user who is having issues with an application. To best understand the issue, the technician simultaneously views the user's screen with the user. Which of the following would BEST accomplish this task?

- A . SSH
- B . VPN
- C . VNC
- D . RDP

---

**Answer: C**

---

Explanation:

VNC (Virtual Network Computing) is a protocol that allows a technician to simultaneously view and control a user's screen remotely. VNC uses a server-client model, where the user's computer runs a VNC server and the technician's computer runs a VNC client. VNC can work across different platforms and operating systems.3. SSH (Secure Shell) is a protocol that allows a technician to access a user's command-line interface remotely, but not their graphical user interface. VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection over a public network, but does not allow screen sharing. RDP (Remote Desktop Protocol) is a protocol that allows a technician to access a user's desktop remotely, but not simultaneously with the user.

---

### Question: 482

---

After a failed update, an application no longer launches and generates the following error message: Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

- A . Device Manager
- B . Administrator Tools
- C . Programs and Features
- D . Recovery

---

**Answer: D**

---

Explanation:

Recovery is a Windows 10 utility that can be used to address the concern of a failed update that prevents an application from launching. Recovery allows the user to reset the PC, go back to a previous version of Windows, or use advanced startup options to troubleshoot and repair the system.2. Device Manager, Administrator Tools, and Programs and Features are not Windows 10 utilities that can fix a failed update.

---

### **Question: 483**

---

A data center is required to destroy SSDs that contain sensitive information. Which of the following is the BEST method to use for the physical destruction of SSDs?

- A . Wiping
- B . Low-level formatting
- C . Shredding
- D . Erasing

---

**Answer: C**

---

Explanation:

[Shredding is the best method to use for the physical destruction of SSDs because it reduces them to small pieces that cannot be recovered or accessed. Wiping, low-level formatting, and erasing are not effective methods for destroying SSDs because they do not physically damage the flash memory chips that store data1.](#)

---

### **Question: 484**

---

A technician is editing the hosts file on a few PCs in order to block certain domains. Which of the following would the technician need to execute after editing the hosts file?

- A . Enable promiscuous mode.
- B . Clear the browser cache.
- C . Add a new network adapter.
- D . Reset the network adapter.

---

**Answer: D**

---

Explanation:

[Resetting the network adapter is the best way to apply the changes made to the hosts file on a few PCs. The hosts file is a text file that maps hostnames to IP addresses and can be used to block certain domains by redirecting them to invalid or local addresses. Resetting the network adapter will clear the DNS cache and force the PC to use the new entries in the hosts file.](#)

---

### **Question: 485**

---

The audio on a user's mobile device is inconsistent when the user uses wireless headphones and moves around. Which of the following should a technician perform to troubleshoot the issue?

- A . Verify the Wi-Fi connection status.
- B . Enable the NFC setting on the device.
- C . Bring the device within Bluetooth range.
- D . Turn on device tethering.

---

**Answer: C**

---

Explanation:

Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

---

### **Question: 486**

---

Which of the following should be used to secure a device from known exploits?

- A . Encryption
- B . Remote wipe
- C . Operating system updates
- D . Cross-site scripting

---

**Answer: C**

---

Explanation:

Operating system updates are used to secure a device from known exploits. Operating system updates are patches or fixes that are released by the vendor to address security vulnerabilities, bugs, or performance issues. Operating system updates can also provide new features or enhancements to the device. It is important to keep the operating system updated to prevent attackers from exploiting known flaws or weaknesses.

---

### **Question: 487**

---

Which of the following macOS features provides the user with a high-level view of all open windows?

- A . Mission Control
- B . Finder
- C . Multiple Desktops
- D . Spotlight

---

**Answer: A**

---

Explanation:

Mission Control is the macOS feature that provides the user with a high-level view of all open windows. Mission Control allows the user to see and switch between multiple desktops, full-screen apps, and windows in a single screen. Mission Control can be accessed by swiping up with three or four fingers on the trackpad, pressing F3 on the keyboard, or moving the cursor to a hot corner

---

### Question: 488

---

A company acquired a local office, and a technician is attempting to join the machines at the office to the local domain. The technician notes that the domain join option appears to be missing. Which of the following editions of Windows is MOST likely installed on the machines?

- A . Windows Professional
- B . Windows Education
- C . Windows Enterprise
- D . Windows Home

---

**Answer: D**

---

Explanation:

Windows Home is the most likely edition of Windows installed on the machines that do not have the domain join option. Windows Home is a consumer-oriented edition that does not support joining a domain or using Group Policy. Only Windows Professional, Education, and Enterprise editions can join a domain

---

### Question: 489

---

An organization implemented a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. Which of the following wireless security methods BEST describes what this organization implemented?

- A . TKIP
- B . RADIUS
- C . WPA2
- D . AES

---

**Answer: B**

---

Explanation:

RADIUS stands for Remote Authentication Dial-In User Service and it is a protocol that provides centralized authentication, authorization, and accounting for network access. RADIUS can be used to implement a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. This is also known as 802.1X authentication or EAP-TLS authentication

---

## **Question: 490**

---

A technician installed a new application on a workstation. For the program to function properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?

- A . System
- B . Indexing Options
- C . Device Manager
- D . Programs and Features

---

**Answer: A**

---

Explanation:

[System is the Control Panel utility that should be used to change the Path Environment Variable. The Path Environment Variable is a system variable that specifies the directories where executable files are located. To edit the Path Environment Variable, the technician should go to System > Advanced system settings > Environment Variables and then select Path from the list of system variables and click Edit.](#)

---

## **Question: 491**

---

Which of the following is used to integrate Linux servers and desktops into Windows Active Directory environments?

- A . apt-get
- B . CIFS
- C . Samba
- D . grep

---

**Answer: C**

---

Explanation:

[Samba is a software suite that allows Linux servers and desktops to integrate with Windows Active Directory environments. Samba can act as a domain controller, a file server, a print server, or a client for Windows networks. Samba can also provide authentication and authorization services for Linux users and devices using Active Directory.](#)

---

## **Question: 492**

---

While staying at a hotel, a user attempts to connect to the hotel Wi-Fi but notices that multiple SSIDs have very similar names. Which of the following social-engineering attacks is being attempted?

- A . Evil twin
- B . Impersonation
- C . Insider threat

---

**Answer: A**

---

Explanation:

An evil twin is a type of social-engineering attack that involves setting up a rogue wireless access point that mimics a legitimate one. The attacker can then intercept or modify the traffic of the users who connect to the fake SSID. The attacker may also use phishing or malware to steal credentials or personal information from the users

---

### **Question: 493**

---

Which of the following would MOST likely be used to change the security settings on a user's device in a domain environment?

- A . Security groups
- B . Access control list
- C . Group Policy
- D . Login script

---

**Answer: C**

---

Explanation:

Group Policy is the most likely tool to be used to change the security settings on a user's device in a domain environment. Group Policy is a feature of Windows that allows administrators to manage and configure settings for multiple devices and users in a centralized way. Group Policy can be used to enforce security policies such as password complexity, account lockout, firewall rules, encryption settings, etc.

---

### **Question: 494**

---

A technician is installing a program from an ISO file. Which of the following steps should the technician take?

- A . Mount the ISO and run the installation file.
- B . Copy the ISO and execute on the server.
- C . Copy the ISO file to a backup location and run the ISO file.
- D . Unzip the ISO and execute the setup.exe file.

---

**Answer: A**

---

Explanation:

Mounting the ISO and running the installation file is the correct way to install a program from an ISO file. An ISO file is an image of a disc that contains all the files and folders of a program. Mounting the ISO means creating a virtual

drive that can access the ISO file as if it were a physical disc. Running the installation file means executing the setup program that will install the program on the computer

---

### Question: 495

---

All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

- A . Rolling back video card drivers
- B . Restoring the PC to factory settings
- C . Repairing the Windows profile
- D . Reinstalling the Windows OS

---

**Answer: A**

---

Explanation:

Rolling back video card drivers is the best way to resolve the issue of large desktop icons on a user's newly issued PC. This means restoring the previous version of the drivers that were working fine before the software patch was deployed. The software patch may have caused compatibility issues or corrupted the drivers, resulting in display problems

---

### Question: 496

---

A customer calls a service support center and begins yelling at a technician about a feature for a product that is not working to the customer's satisfaction. This feature is not supported by the service support center and requires a field technician to troubleshoot. The customer continues to demand service. Which of the following is the BEST course of action for the support center representative to take?

- A . Inform the customer that the issue is not within the scope of this department.
- B . Apologize to the customer and escalate the issue to a manager.
- C . Ask the customer to explain the issue and then try to fix it independently.
- D . Respond that the issue is something the customer should be able to fix.

---

**Answer: B**

---

Explanation:

Apologizing to the customer and escalating the issue to a manager is the best course of action for the support center representative to take. This shows empathy and professionalism and allows the manager to handle the situation and provide the appropriate service or resolution for the customer.

---

### **Question: 497**

---

Which of the following options should MOST likely be considered when preserving data from a hard drive for forensic analysis? (Select TWO).

- A . Licensing agreements
- B . Chain of custody
- C . Incident management documentation
- D . Data integrity
- E . Material safety data sheet
- F . Retention requirements

---

**Answer: B**

---

Explanation:

Chain of custody and data integrity are two options that should most likely be considered when preserving data from a hard drive for forensic analysis. Chain of custody refers to the documentation and tracking of who has access to the data and how it is handled, stored, and transferred. Data integrity refers to the assurance that the data has not been altered, corrupted, or tampered with during the preservation process

---

### **Question: 498**

---

A manager called the help desk to ask for assistance with creating a more secure environment for the finance department- which resides in a non-domain environment. Which of the following would be the BEST method to protect against unauthorized use?

- A . Implementing password expiration
- B . Restricting user permissions
- C . Using screen locks
- D . Disabling unnecessary services

---

**Answer: B**

---

Explanation:

Restricting user permissions is a method of creating a more secure environment for the finance department in a non-domain environment. This means that users will only have access to the files and resources that they need to perform their tasks and will not be able to modify or delete other files or settings that could compromise security or functionality.

---

### **Question: 499**

---

A user is no longer able to start the OS on a computer and receives an error message indicating there is no OS found. A technician reviews the audit logs and notes that the user's system posted a S.M.A.R.T. error just days before this

issue. Which of the following is the MOST likely cause of this issue?

- A . Boot order
- B . Malware
- C . Drive failure
- D . Windows updates

---

**Answer: C**

---

Explanation:

A S.M.A.R.T. error is a warning that a hard drive is about to fail or has failed. This means that the OS cannot be loaded from the drive and the user will see an error message indicating there is no OS found. The most likely cause of this issue is drive failure.

---

### **Question: 500**

---

A technician is finalizing a new workstation for a user. The user's PC will be connected to the internet but will not require the same private address each time. Which of the following protocols will the technician MOST likely utilize?

- A . DHCP
- B . SMTP
- C . DNS
- D . RDP

---

**Answer: A**

---

Explanation:

DHCP stands for Dynamic Host Configuration Protocol and it is used to assign IP addresses and other network configuration parameters to devices on a network automatically. This is useful for devices that do not require the same private address each time they connect to the internet.

---

### **Question: 501**

---

A user contacts a technician about an issue with a laptop. The user states applications open without being launched and the browser redirects when trying to go to certain websites. Which of the following is MOST likely the cause of the user's issue?

- A . Keylogger
- B . Cryptominers
- C . Virus
- D . Malware

---

**Answer: D**

---

Explanation:

The most likely cause of the user's issue of applications opening without being launched and browser redirects when trying to go to certain websites is malware. Malware is a general term that refers to any software or code that is malicious or harmful to a computer or system. Malware can perform various unwanted or unauthorized actions on a computer or system, such as opening applications, redirecting browsers, displaying ads, stealing data, encrypting files or damaging hardware. Malware can infect a computer or system through various means, such as email attachments, web downloads, removable media or network connections. Keylogger is a type of malware that records and transmits the keystrokes made by a user on a keyboard. Keylogger can be used to steal personal or sensitive information, such as passwords, credit card numbers or chat messages. Keylogger does not typically open applications or redirect browsers but only captures user inputs. Cryptominers are a type of malware that use the computing resources of a computer or system to mine cryptocurrency, such as Bitcoin or Ethereum. Cryptominers can degrade the performance and increase the power consumption of a computer or system. Cryptominers do not typically open applications or redirect browsers but only consume CPU or GPU cycles. Virus is a type of malware that infects and replicates itself on other files or programs on a computer or system.

---

**Question: 502**

---

An implementation specialist is replacing a legacy system at a vendor site that has only one wireless network available. When the specialist connects to Wi-Fi, the specialist realizes the insecure network has open authentication. The technician needs to secure the vendor's sensitive data.

- a. Which of the following should the specialist do FIRST to protect the company's data?
- A . Manually configure an IP address, a subnet mask, and a default gateway.
- B . Connect to the vendor's network using a VPN.
- C . Change the network location to private.
- D . Configure MFA on the network.

---

**Answer: B**

---

Explanation:

The first thing that the specialist should do to protect the company's data on an insecure network with open authentication is to connect to the vendor's network using a VPN. A VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public or untrusted network. A VPN can protect the company's data by preventing eavesdropping, interception or modification of the network traffic by unauthorized parties. A VPN can also provide access to the company's internal network and resources remotely. Manually configuring an IP address, a subnet mask and a default gateway may not be necessary or possible if the vendor's network uses DHCP to assign network configuration parameters automatically. Manually configuring an IP address, a subnet mask and a default gateway does not protect the company's data from network attacks or threats. Changing the network location to private may not be advisable or effective if the vendor's network is a public or untrusted network. Changing the network location to private does not protect the company's data from network attacks or threats. Configuring MFA on the network may not be feasible or sufficient if the vendor's network has open authentication and does not support or require MFA. Configuring MFA on the network does not protect the

---

### Question: 503

---

A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

- A . Private-browsing mode
- B . Invalid certificate
- C . Modified file
- D . Browser cache

---

**Answer: C**

---

Explanation:

The most likely cause of the issue of having different hash values for a downloaded security tool is a modified file. A hash value is a unique and fixed-length string that is generated from an algorithm that processes data or files. A hash value can be used to verify the integrity and authenticity of data or files by comparing it with a known or expected value. If the hash values do not match, it means that the data or file has been altered or corrupted in some way. A modified file may result from intentional or unintentional changes, such as editing, encryption, compression or malware infection. Private-browsing mode is a feature that allows users to browse the web without storing any browsing history, cookies or cache on their browser. Private-browsing mode does not affect the hash value of a downloaded file but only how the browser handles user data. Invalid certificate is an error that occurs when a website or a server does not have a valid or trusted digital certificate that proves its identity and secures its communication. Invalid certificate does not affect the hash value of a downloaded file but only how the browser verifies the website or server's credibility. Browser cache is a temporary storage that stores copies of web pages, images and other content that users have visited on their browser.

---

### Question: 504

---

A technician is troubleshooting a mobile device that was dropped. The technician finds that the screen (fails to rotate, even though the settings are correctly applied. Which of the following pieces of hardware should the technician replace to resolve the issue?

- A . LCD
- B . Battery
- C . Accelerometer
- D . Digitizer

---

**Answer: C**

---

Explanation:

The piece of hardware that the technician should replace to resolve the issue of the screen failing to rotate on a mobile device that was dropped is the accelerometer. The accelerometer is a sensor that detects the orientation and movement of the mobile device by measuring the acceleration forces acting on it. The accelerometer allows the screen to rotate automatically according to the position and angle of the device. If the accelerometer is damaged or malfunctioning, the screen may not rotate properly or at all, even if the settings are correctly applied. LCD stands for Liquid Crystal Display and is a type of display that uses liquid crystals and backlight to produce images on the screen. LCD is not related to the screen rotation feature but to the quality and brightness of the display. Battery is a component that provides power to the mobile device by storing and releasing electrical energy. Battery is not related to the screen rotation feature but to the battery life and performance of the device. Digitizer is a component that converts touch inputs into digital signals that can be processed by the mobile device. Digitizer is not related to the screen rotation feature but to the touch sensitivity and accuracy of the display. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.5

---

### Question: 505

---

Which of the following filesystem formats would be the BEST choice to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems?

- A . APFS
- B . ext4
- C . CDFS
- D . FAT32

---

**Answer: D**

---

Explanation:

The best filesystem format to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems is FAT32. FAT32 stands for File Allocation Table 32-bit and is a filesystem format that organizes and manages files and folders on storage devices using 32-bit clusters. FAT32 is compatible with most Microsoft operating systems since Windows 95 OSR2, as well as other operating systems such as Linux and Mac OS X. FAT32 can support storage devices up to 2TB in size and files up to 4GB in size. APFS stands for Apple File System and is a filesystem format that organizes and manages files and folders on storage devices using encryption, snapshots and cloning features. APFS is compatible with Mac OS X 10.13 High Sierra and later versions but not with Microsoft operating systems natively. Ext4 stands for Fourth Extended File System and is a filesystem format that organizes and manages files and folders on storage devices using journaling, extents and delayed allocation features. Ext4 is compatible with Linux operating systems but not with Microsoft operating systems natively.

---

### Question: 506

---

Which of the following defines the extent of a change?

- A . Scope
- B . Purpose
- C . Analysis
- D . Impact

Explanation:

The term that defines the extent of a change is scope. Scope is a measure of the size, scale and boundaries of a project or an activity. Scope defines what is included and excluded in the project or activity, such as goals, requirements, deliverables, tasks and resources. Scope helps determine the feasibility, duration and cost of the project or activity. Scope also helps manage the expectations and needs of the stakeholders involved in the project or activity. Purpose is the reason or objective for doing a project or an activity. Purpose defines why the project or activity is important or necessary, such as solving a problem, meeting a need or achieving a goal. Purpose helps provide direction, motivation and justification for the project or activity. Analysis is the process of examining, evaluating and interpreting data or information related to a project or an activity. Analysis helps identify, understand and prioritize issues, risks, opportunities and solutions for the project or activity. Impact is the effect or outcome of a project or an activity on something or someone else. Impact defines how the project or activity affects or influences other factors, such as performance, quality, satisfaction or value. Impact helps measure the success and effectiveness of the project or activity. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.2

---

**Question: 507**

---

Which of the following features allows a technician to configure policies in a Windows 10 Professional desktop?

- A . gpedit
- B . gpmc
- C . gpresult
- D . gpupdate

Explanation:

The feature that allows a technician to configure policies in a Windows 10 Professional desktop is gpedit. Gpedit is a command that opens the Local Group Policy Editor, which is a utility that allows users to view and modify local group policies on their Windows PC. Local group policies are a set of rules and settings that control the behavior and configuration of the system and its users. Local group policies can be used to configure policies such as security, network, software installation and user rights. Gpmc is a command that opens the Group Policy Management Console, which is a utility that allows users to view and modify domain-based group policies on a Windows Server. Domain-based group policies are a set of rules and settings that control the behavior and configuration of the computers and users in a domain. Domain-based group policies are not available on a Windows 10 Professional desktop. Gpresult is a command that displays the result of applying group policies on a Windows PC. Gpresult can be used to troubleshoot or verify group policy settings but not to configure them. Gpupdate is a command that updates or refreshes the group policy settings on a Windows PC. Gpupdate can be used to apply new or changed group policy settings but not to configure them. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

---

## **Question: 508**

---

A technician needs to add an individual as a local administrator on a Windows home PC. Which of the following utilities would the technician MOST likely use?

- A . Settings > Personalization
- B . Control Panel > Credential Manager
- C . Settings > Accounts > Family and Other Users
- D . Control Panel > Network and Sharing Center

---

**Answer: C**

---

Explanation:

The technician would most likely use Settings > Accounts > Family and Other Users to add an individual as a local administrator on a Windows home PC. Settings > Accounts > Family and Other Users allows users to add and manage other user accounts on their Windows PC. The technician can add an individual as a local administrator by selecting Add someone else to this PC under Other users and following the steps to create a new user account with administrator privileges. Settings > Personalization allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. Settings > Personalization is not related to adding an individual as a local administrator on a Windows home PC but to configuring desktop settings and preferences. Control Panel > Credential Manager allows users to view and manage their web credentials and Windows credentials stored on their Windows PC. Control Panel > Credential Manager is not related to adding

---

## **Question: 509**

---

Which of the following is the default GUI and file manager in macOS?

- A . Disk Utility
- B . Finder
- C . Dock
- D . FileVault

---

**Answer: B**

---

Explanation:

Finder is the default GUI and file manager in macOS. Finder is an application that allows users to access and manage files and folders on their Mac computers. Finder also provides features such as Quick Look, Spotlight, AirDrop and iCloud Drive. Finder uses a graphical user interface that consists of icons, menus, toolbars and windows to display and interact with files and folders. Disk Utility is a utility that allows users to view and manage disk drives and partitions on their Mac computers. Disk Utility is not a GUI or a file manager but a disk management tool. Dock is a feature that allows users to access and launch applications on their Mac computers. Dock is not a GUI or a file manager but an application launcher. FileVault is a feature that allows users to encrypt and protect their data on their Mac computers. FileVault is not a GUI or a file manager but an encryption tool. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.1

---

## **Question: 510**

---

A Windows workstation that was recently updated with approved system patches shut down instead of restarting. Upon reboot, the technician notices an alert stating the workstation has malware in the root OS folder. The technician promptly performs a System Restore and reboots the workstation, but the malware is still detected. Which of the following BEST describes why the system still has malware?

- A . A system patch disabled the antivirus protection and host firewall.
- B . The system updates did not include the latest anti-malware definitions.
- C . The system restore process was compromised by the malware.
- D . The malware was installed before the system restore point was created.

---

**Answer: D**

---

Explanation:

The best explanation for why the system still has malware after performing a System Restore is that the malware was installed before the system restore point was created. A system restore point is a snapshot of the system settings and configuration at a certain point in time. A System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, a System Restore does not affect personal files or folders, and it may not remove malware that was already present on the system before the restore point was created. A system patch disabling the antivirus protection and host firewall may increase the risk of malware infection, but it does not explain why the malware persists after a System Restore. The system updates not including the latest anti-malware definitions may reduce the effectiveness of malware detection and removal, but it does not explain why the malware persists after a System Restore. The system restore process being compromised by the malware may prevent a successful System Restore, but it does not explain why the malware persists after a System Restore. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.3

---

## **Question: 511**

---

A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?

- A . The system is missing updates.
- B . The system is utilizing a 32-bit OS.
- C . The system's memory is failing.
- D . The system requires BIOS updates

---

**Answer: B**

---

Explanation:

The most likely reason that the system is not utilizing all the available RAM is that the system is utilizing a 32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit

OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes. A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64-bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.1

---

### Question: 512

---

A user calls the help desk to report that Windows installed updates on a laptop and rebooted overnight. When the laptop started up again, the touchpad was no longer working. The technician thinks the software that controls the touchpad might be the issue. Which of the following tools should the technician use to make adjustments?

- A . eventvwr.msc
- B . perfmon.msc
- C . gpedit.msc
- D . devmgmt.msc

---

**Answer: D**

---

Explanation:

The technician should use devmgmt.msc tool to make adjustments for the touchpad issue after Windows installed updates on a laptop. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the touchpad device and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the touchpad issue, but it does not allow users to manage or troubleshoot the device or its driver directly. Perfmon.msc is a command that opens the Performance Monitor, which is a utility that allows users to measure and analyze the performance of the system

---

### Question: 513

---

A kiosk, which is running Microsoft Windows 10, relies exclusively on a numeric keypad to allow customers to enter their ticket numbers but no other information. If the kiosk is idle for four hours, the login screen locks. Which of the following sign-on options would allow any employee the ability to unlock the kiosk?

- A . Requiring employees to enter their usernames and passwords
- B . Setting up facial recognition for each employee
- C . Using a PIN and providing it to employees
- D . Requiring employees to use their fingerprints

Explanation:

The best sign-on option that would allow any employee the ability to unlock the kiosk that relies exclusively on a numeric keypad is to use a PIN and provide it to employees. A PIN is a Personal Identification Number that is a numeric code that can be used as part of authentication or access control. A PIN can be entered using only a numeric keypad and can be easily shared with employees who need to unlock the kiosk. Requiring employees to enter their usernames and passwords may not be feasible or convenient if the kiosk only has a numeric keypad and no other input devices. Setting up facial recognition for each employee may not be possible or secure if the kiosk does not have a camera or biometric sensor. Requiring employees to use their fingerprints may not be possible or secure if the kiosk does not have a fingerprint scanner or biometric sensor. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

---

**Question: 514**

---

Which of the following only has a web browser interface?

- A . Linux
- B . Microsoft Windows
- C . iOS
- D . Chromium

Explanation:

Chromium is an operating system that only has a web browser interface. Chromium is an open-source project that provides the source code and framework for Chrome OS, which is a Linux-based operating system developed by Google. Chromium and Chrome OS are designed to run web applications and cloud services through the Chrome web browser, which is the only user interface available on the system. Chromium and Chrome OS are mainly used on devices such as Chromebooks, Chromeboxes and Chromebits. Linux is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Linux is an open-source and customizable operating system that can run various applications and services on different devices and platforms. Linux can also support different web browsers, such as Firefox, Opera and Chromium. Microsoft Windows is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Microsoft Windows is a proprietary and popular operating system that can run various applications and services on different devices and platforms. Microsoft Windows can also support different web browsers, such as Edge, Internet Explorer and Chrome. iOS is an operating system that does not only have a web browser interface but also a graphical user interface and a voice-based interface. iOS is a proprietary and mobile operating system developed by Apple that can run various applications and services on devices such as iPhone, iPad and iPod Touch. iOS can also support different web browsers, such as Safari, Firefox and Chrome. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

---

## **Question: 515**

---

A user added a second monitor and wants to extend the display to it. In which of the following Windows settings will the user MOST likely be able to make this change?

- A . System
- B . Devices
- C . Personalization
- D . Accessibility

---

**Answer: A**

---

Explanation:

The user can most likely make the change of extending the display to a second monitor in the System option in the Windows settings. The System option allows users to manage system settings and features, such as display, sound, notifications, power and storage. The user can extend the display to a second monitor by selecting Display from the System option and then choosing Extend these displays from the Multiple displays drop-down menu. This will allow the user to use both monitors as one large desktop area. Devices is an option in the Windows settings that allows users to add and manage devices connected to the computer, such as printers, scanners, mice and keyboards. Devices is not related to extending the display to a second monitor but to configuring device settings and preferences. Personalization is an option in the Windows settings that allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver.

---

## **Question: 516**

---

Which of the following script types is used with the Python language by default?

- A .ps1
- B .vbs
- C .bat
- D .py

---

**Answer: D**

---

Explanation:

The script type that is used with the Python language by default is .py. .py is a file extension that indicates a Python script file that contains Python code that can be executed by a Python interpreter or compiler. Python is a high-level, general-purpose and interpreted programming language that can be used for various applications, such as web development, data analysis, machine learning and automation. .ps1 is a file extension that indicates a PowerShell script file that contains PowerShell code that can be executed by a PowerShell interpreter or compiler. PowerShell is a task-based, command-line and scripting language that can be used for system administration and automation on Windows systems. .vbs is a file extension that indicates a VBScript file that contains VBScript code that can be executed by a VBScript interpreter or compiler. VBScript is an Active Scripting language that can be used for web development and automation on Windows systems. .bat is a file extension that indicates a batch file that contains a series of commands that can be executed by a command-line interpreter or shell on Windows systems. Batch files

---

### Question: 517

---

A user has been unable to receive emails or browse the internet from a smartphone while traveling. However, text messages and phone calls are working without issue. Which of the following should a support technician check FIRST?

- A . User account status
- B . Mobile OS version
- C . Data plan coverage
- D . Network traffic outages

---

**Answer: C**

---

Explanation:

The first thing that a support technician should check to resolve the issue of not being able to receive emails or browse the internet from a smartphone while traveling is the data plan coverage. The data plan coverage determines how much data and where the user can use on the smartphone's cellular network. The data plan coverage may vary depending on the user's location, carrier and subscription. The data plan coverage may not include or support certain areas or countries that the user is traveling to, or may charge extra fees or limit the speed or amount of data that the user can use. The data plan coverage does not affect text messages and phone calls, which use different network services and protocols. User account status is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the user account has been suspended or terminated by the carrier or the email provider. Mobile OS version is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the mobile OS has a major bug or compatibility problem with the network or the email app. Network traffic outages may cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, but they are less likely and less common than data plan coverage issues, and they should also affect text messages and phone calls. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

---

### Question: 518

---

A user calls the help desk to report that mapped drives are no longer accessible. The technician verifies that clicking on any of the drives on the user's machine results in an error message. Other users in the office are not having any issues. As a first step, the technician would like to remove and attempt to reconnect the drives. Which of the following command-line tools should the technician use?

- A . net use
- B . set
- C . mkdir
- D . rename

---

**Answer: A**

---

Explanation:

The technician should use net use command-line tool to remove and reconnect mapped drives. Net use is a command that allows users to manage network connections and resources, such as shared folders or printers. Net use can be used to map or unmap network drives by specifying their drive letters and network paths. For example, net use Z: \server\share maps drive Z: to \server\share folder, and net use Z: /delete unmaps drive Z:. Set is a command that displays or modifies environment variables for the current user or process. Set is not related to managing mapped drives. Mkdir is a command that creates a new directory or folder in the current or specified location. Mkdir is not related to managing mapped drives. Rename is a command that renames a file or folder in the current or specified location. Rename is not related to managing mapped drives. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

---

**Question: 519**

---

A technician is securing a new Windows 10 workstation and wants to enable a Screensaver lock. Which of the following options in the Windows settings should the technician use?

- A . Ease of Access
- B . Privacy
- C . Personalization
- D . Update and Security

---

**Answer: C**

---

Explanation:

The technician should use the Personalization option in the Windows settings to enable a Screensaver lock. The Personalization option allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. The technician can enable a Screensaver lock by choosing a screensaver from the drop-down menu, setting a wait time in minutes and checking the box that says "On resume, display logon screen". This will lock the computer and require a password or PIN to log back in after the screensaver is activated. Ease of Access is an option in the Windows settings that allows users to adjust accessibility features and settings, such as narrator, magnifier, high contrast and keyboard shortcuts. Ease of Access is not related to enabling a Screensaver lock. Privacy is an option in the Windows settings that allows users to manage privacy and security settings, such as location, camera, microphone and app permissions. Privacy is not related to enabling a Screensaver lock. Update and Security is an option in the Windows settings that allows users to check and install updates, troubleshoot problems, backup files and restore system. Update and Security is not related to enabling a Screensaver lock. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.7

---

**Question: 520**

---

A Windows user recently replaced a computer. The user can access the public internet on the computer; however, an internal site at <https://companyintranet.com:8888> is no longer loading. Which of the following should a technician adjust to resolve the issue?

- A . Default gateway settings
- B . DHCP settings
- C . IP address settings
- D . Firewall settings
- E . Antivirus settings

---

**Answer: D**

---

Explanation:

The technician should adjust the firewall settings to resolve the issue of not being able to access an internal site at <https://companyintranet.com:8888>. The firewall settings control how the firewall filters and allows network traffic based on rules and policies. The firewall settings may be blocking or preventing the access to the internal site by mistake or by default, especially if the site uses a non-standard port number such as 8888. The technician should check and modify the firewall settings to allow the access to the internal site or its port number. Default gateway settings determine how a computer connects to other networks or the internet. Default gateway settings are not likely to cause the issue of not being able to access an internal site if the user can access the public internet. DHCP settings determine how a computer obtains its IP address and other network configuration parameters automatically from a DHCP server. DHCP settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. IP address settings determine how a computer identifies itself and communicates with other devices on a network. IP address settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. Antivirus settings control how the antivirus software scans and protects the computer from malware and threats. Antivirus settings are less likely to cause the issue of not being able to access an internal site than firewall settings, unless the antivirus software has its own firewall feature that may interfere with the network traffic. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

---

### **Question: 521**

---

A user reports that the pages flash on the screen two or three times before finally staying open when attempting to access banking web pages. Which of the following troubleshooting steps should the technician perform NEXT to resolve the issue?

- A . Examine the antivirus logs.
- B . Verify the address bar URL.
- C . Test the internet connection speed.
- D . Check the web service status.

---

**Answer: B**

---

Explanation:

The next troubleshooting step that the technician should perform to resolve the issue of pages flashing on the screen before staying open when accessing banking web pages is to verify the address bar URL. The address bar URL is the

web address that appears in the browser's address bar and indicates the location of the web page being accessed. Verifying the address bar URL can help determine if the user is accessing a legitimate or malicious website, as some phishing websites may try to impersonate banking websites by using similar-looking URLs or domains.

---

### **Question: 522**

---

A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?

- A . EULA
- B . PII
- C . DRM
- D . Open-source agreement

---

### **Answer: A**

---

Explanation:

The installation of home edition software on computers at a local office most likely violates the EULA. EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non-commercial purposes only, and prohibit the use of home edition software in business or professional settings. Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open-source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

---

### **Question: 523**

---

A user is trying to use a third-party USB adapter but is experiencing connection issues. Which of the following tools should the technician use to resolve this issue?

- A . taskschd.msc
- B . eventvwr.msc
- C . de vmgmt. msc
- D . diskmgmt.msc

**Explanation:**

The tool that the technician should use to resolve the connection issues with the third-party USB adapter is devmgmt.msc. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the USB adapter and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Taskschd.msc is a command that opens the Task Scheduler, which is a utility that allows users to create and manage tasks that run automatically at specified times or events. The Task Scheduler is not relevant or useful for resolving connection issues with the USB adapter. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the connection issues with the USB adapter, but it does not allow users to manage or troubleshoot the device or its driver directly. Diskmgmt.msc is a command that opens the Disk Management, which is a utility that allows users to view and manage the disk drives and partitions on a computer. The Disk Management is not relevant or useful for resolving connection issues with the USB adapter. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

---

**Question: 524**

---

A user receives a call from someone who claims to be from the user's bank and requests information to ensure the user's account is safe. Which of the following social-engineering attacks is the user experiencing?

- A . Phishing
- B . Smishing
- C . Whaling
- D . Vishing

**Explanation:**

The user is experiencing a vishing attack. Vishing stands for voice phishing and is a type of social-engineering attack that uses phone calls or voice messages to trick users into revealing personal or financial information. Vishing attackers often pretend to be from legitimate organizations, such as banks, government agencies or service providers, and use various tactics, such as urgency, fear or reward, to persuade users to comply with their requests. Phishing is a type of social-engineering attack that uses fraudulent emails or websites to trick users into revealing personal or financial information. Phishing does not involve phone calls or voice messages. Smishing is a type of social-engineering attack that uses text messages or SMS to trick users into revealing personal or financial information. Smishing does not involve phone calls or voice messages. Whaling is a type of social-engineering attack that targets high-profile individuals, such as executives, celebrities or politicians, to trick them into revealing personal or financial information. Whaling does not necessarily involve phone calls or voice messages. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.1

---

## **Question: 525**

---

A technician needs to remotely connect to a Linux desktop to assist a user with troubleshooting. The technician needs to make use of a tool natively designed for Linux. Which of the following tools will the technician MOST likely use?

- A . VNC
- B . MFA
- C . MSRA
- D . RDP

---

## **Answer: A**

---

Explanation:

The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi-Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

---

## **Question: 526**

---

A technician is troubleshooting an issue with a computer that contains sensitive information. The technician determines the computer needs to be taken off site for repair. Which of the following should the technician do NEXT?

- A . Remove the HDD and then send the computer for repair.
- B . Check corporate policies for guidance.
- C . Delete the sensitive information before the computer leaves the building.
- D . Get authorization from the manager.

---

## **Answer: D**

---

Explanation:

The next step that the technician should do before taking the computer off site for repair is to get authorization from the manager. Getting authorization from the manager is important because it ensures that the technician has permission and approval to remove the computer from the premises and perform the repair work off site. Getting

authorization from the manager can also help document and communicate the reason and duration of the repair and avoid any misunderstanding or conflict with the user or the organization. Removing the HDD and then sending the computer for repair may not be feasible or necessary if the issue is not related to the HDD or if the HDD contains essential data or software for the repair. Checking corporate policies for guidance may be a good step but it does not replace getting authorization from the manager who is responsible for the computer and its data. Deleting the sensitive information before the computer leaves the building may not be possible or advisable if the issue prevents access to the data or if the data is needed for troubleshooting or recovery purposes. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

---

### Question: 527

---

Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

- A . Multifactor authentication
- B . Badge reader
- C . Personal identification number
- D . Firewall
- E . Motion sensor
- F . Soft token

---

**Answer: B, E**

---

Explanation:

Badge reader and motion sensor are devices that can be deployed to enhance physical security for a building. A badge reader is a device that scans and verifies an identification card or tag that grants access to authorized personnel only. A badge reader can help prevent unauthorized entry or intrusion into a building or a restricted area. A motion sensor is a device that detects movement and triggers an alarm or an action when motion is detected. A motion sensor can help deter or alert potential intruders or trespassers in a building or an area. Multifactor authentication is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. Multifactor authentication is not a device that can be deployed to enhance physical security for a building but a technique that can be used to enhance logical security for systems or services. Personal identification number is a numeric code that can be used as part of authentication or access control. Personal identification number is not a device that can be deployed to enhance physical security for a building but an example of something you know factor in multifactor authentication. Firewall is a device or software that filters network traffic based on rules and policies. Firewall is not a device that can be deployed to enhance physical security for a building but a device that can be used to enhance network security for systems or services. Soft token is an application or software that generates one-time passwords or codes for authentication purposes. Soft token is not a device that can be deployed to enhance physical security for a building but an example of something you have factor in multifactor authentication. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

---

### Question: 528

---

Which of the following is used to explain issues that may occur during a change implementation?

- A . Scope change
- B . End-user acceptance
- C . Risk analysis
- D . Rollback plan

---

**Answer: C**

---

Explanation:

Risk analysis is used to explain issues that may occur during a change implementation. Risk analysis is a process of identifying, assessing and prioritizing potential risks that may affect a project or an activity. Risk analysis can help determine the likelihood and impact of various issues that may arise during a change implementation, such as technical errors, compatibility problems, security breaches, performance degradation or user dissatisfaction. Risk analysis can also help plan and prepare for mitigating or avoiding these issues. Scope change is a modification of the original goals, requirements or deliverables of a project or an activity. Scope change is not used to explain issues that may occur during a change implementation but to reflect changes in expectations or needs of the stakeholders. End-user acceptance is a measure of how well the users are satisfied with and adopt a new system or service. End-user acceptance is not used to explain issues that may occur during a change implementation but to evaluate the success and effectiveness of the change. Rollback plan is a contingency plan that describes how to restore a system or service to its previous state in case of a failed or problematic change implementation. Rollback plan is not used to explain issues that may occur during a change implementation but to recover from them. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

---

### **Question: 529**

---

A user lost a company tablet that was used for customer intake at a doctor's office. Which of the following actions would BEST protect against unauthorized access of the data?

- A . Changing the office's Wi-Fi SSID and password
- B . Performing a remote wipe on the device
- C . Changing the user's password
- D . Enabling remote drive encryption

---

**Answer: B**

---

Explanation:

The best action to protect against unauthorized access of the data on the lost company tablet is to perform a remote wipe on the device. A remote wipe is a feature that allows an administrator or a user to erase all the data and settings on a device remotely, usually through a web portal or an email command. A remote wipe can help prevent the data from being accessed or compromised by anyone who finds or steals the device. Changing the office's Wi-Fi SSID and password may prevent the device from connecting to the office network but may not prevent the data from being accessed locally or through other networks. Changing the user's password may prevent the device from logging in to the user's account but may not prevent the data from being accessed by other means or accounts. Enabling remote drive encryption may protect the data from being read by unauthorized parties but may not be possible if the device is already lost or turned off. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.1

---

### **Question: 530**

---

A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?

- A . MSDS
- B . EULA
- C . UAC
- D . AUP

---

**Answer: D**

---

Explanation:

A new employee will need to sign an AUP before being granted login access to the network. An AUP is an Acceptable Use Policy that defines the rules and guidelines for using network resources and services in an organization. An AUP typically covers topics such as security, privacy, ethics, compliance and liability issues related to network usage. An AUP helps protect the organization and its users from legal, regulatory and reputational risks associated with network activities. An MSDS is a Material Safety Data Sheet that provides information about hazardous substances and how to handle them safely. An MSDS is not related to network access or usage. A EULA is an End User License Agreement that specifies the terms and conditions for using a software product or service. A EULA is usually provided by software vendors or developers and does not apply to network access or usage in general. A UAC is a User Account Control that is a security feature that prompts users for permission or confirmation before performing certain actions that require elevated privileges or affect system settings. A UAC is not a document that needs to be signed by users but a mechanism that helps prevent unauthorized changes or malware infections on a system.

Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

---

### **Question: 531**

---

A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?

- A . Disable System Restore.
- B . Schedule a malware scan.
- C . Educate the end user.
- D . Run Windows Update.

---

**Answer: A**

---

Explanation:

Before removing a Trojan virus from a workstation, a technician should disable System Restore. System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, System Restore can also restore infected files or registry entries that were removed by antivirus software or manual actions. By disabling System Restore, a technician can ensure that the Trojan virus is completely removed and does not

reappear after a system restore operation. Scheduling a malware scan may help detect and remove some malware but may not be effective against all types of Trojan viruses. Educating the end user may help prevent future infections but does not address the current issue of removing the Trojan virus. Running Windows Update may help patch some security vulnerabilities but does not guarantee that the Trojan virus will be removed. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

---

### Question: 532

---

A network technician installed a SOHO router for a home office user. The user has read reports about home routers being targeted by malicious actors and then used in DDoS attacks. Which of the following can the technician MOST likely do to defend against this threat?

- A . Add network content filtering.
- B . Disable the SSID broadcast.
- C . Configure port forwarding.
- D . Change the default credentials.

---

### Answer: D

---

Explanation:

One of the most effective ways to defend against malicious actors targeting home routers for DDoS attacks is to change the default credentials of the router. The default credentials are often well-known or easily guessed by attackers, who can then access and compromise the router settings and firmware. By changing the default credentials to strong and unique ones, a technician can prevent unauthorized access and configuration changes to the router. Adding network content filtering may help block some malicious or unwanted websites but may not prevent attackers from exploiting router vulnerabilities or backdoors. Disabling the SSID broadcast may help reduce the visibility of the wireless network but may not prevent attackers from scanning or detecting it. Configuring port forwarding may help direct incoming traffic to specific devices or services but may not prevent attackers from sending malicious packets or requests to the router. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

---

### Question: 533

---

A user tries to access commonly used web pages but is redirected to unexpected websites. Clearing the web browser cache does not resolve the issue. Which of the following should a technician investigate NEXT to resolve the issue?

- A . Enable firewall ACLs.
- B . Examine the localhost file entries.
- C . Verify the routing tables.
- D . Update the antivirus definitions.

---

### Answer: B

---

Explanation:

A possible cause of the user being redirected to unexpected websites is that the localhost file entries have been modified by malware or hackers to point to malicious or unwanted websites. The localhost file is a text file that maps hostnames to IP addresses and can override DNS settings. By examining the localhost file entries, a technician can identify and remove any suspicious or unauthorized entries that may cause the redirection issue. Enabling firewall ACLs may not resolve the issue if the firewall rules do not block the malicious or unwanted websites. Verifying the routing tables may not resolve the issue if the routing configuration is correct and does not affect the web traffic. Updating the antivirus definitions may help prevent future infections but may not remove the existing malware or changes to the localhost file. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.3

---

### Question: 534

---

A large company is selecting a new Windows operating system and needs to ensure it has built-in encryption and endpoint protection. Which of the following Windows versions will MOST likely be selected?

- A . Home
- B . Pro
- C . Pro for Workstations
- D . Enterprise

---

**Answer: D**

---

Explanation:

When selecting a new Windows operating system for a large company that needs built-in encryption and endpoint protection, the Enterprise edition is the most likely choice. This edition provides advanced security features such as Windows Defender Advanced Threat Protection (ATP), AppLocker, and BitLocker Drive Encryption. These features can help to protect the company's data and endpoints against malware attacks, unauthorized access, and data theft.

The Home and Pro editions of Windows do not include some of the advanced security features provided by the Enterprise edition, such as Windows Defender ATP and AppLocker. The Pro for Workstations edition is designed for high-performance and high-end hardware configurations, but it does not provide additional security features beyond those provided by the Pro edition.

---

### Question: 535

---

Which of the following is the proper way for a technician to dispose of used printer consumables?

- A . Proceed with the custom manufacturer's procedure.
- B . Proceed with the disposal of consumables in standard trash receptacles.
- C . Empty any residual ink or toner from consumables before disposing of them in a standard recycling bin.
- D . Proceed with the disposal of consumables in standard recycling bins.

---

**Answer: A**

---

## Explanation:

When it comes to disposing of used printer consumables, it is important to follow the manufacturer's instructions or guidelines for proper disposal, as different types of consumables may require different disposal procedures. Some manufacturers provide specific instructions for proper disposal, such as sending the used consumables back to the manufacturer or using special recycling programs.

Therefore, the proper way for a technician to dispose of used printer consumables is to proceed with the custom manufacturer's procedure, if provided. This option ensures that the disposal is handled in an environmentally friendly and safe manner.

---

### Question: 536

---

A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. Which of the following will MOST likely resolve the issue?

- A . Recalibrating the magnetometer
- B . Recalibrating the compass
- C . Recalibrating the digitizer
- D . Recalibrating the accelerometer

---

### Answer: D

---

## Explanation:

When a user rotates a cell phone horizontally to read emails and the display remains vertical, even though the settings indicate autorotate is on, this is typically due to a problem with the phone's accelerometer. The accelerometer is the sensor that detects changes in the phone's orientation and adjusts the display accordingly. If the accelerometer is not calibrated correctly, the display may not rotate as expected.

Recalibrating the accelerometer is the most likely solution to this issue. The process for recalibrating the accelerometer can vary depending on the specific device and operating system, but it typically involves going to the device's settings and finding the option to calibrate or reset the sensor. Users may need to search their device's documentation or online resources to find specific instructions for their device.

---

### Question: 537

---

A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?

- A . Convert the PC from a DHCP assignment to a static IP address.
- B . Run a speed test to ensure the advertised speeds are met.
- C . Test all network sharing and printing functionality the customer uses.
- D . Change the default passwords on new network devices.

---

**Answer: D**

---

Explanation:

When a homeowner moves and sets up a new router for the new ISP it is important to take appropriate security measures to protect their network from potential security threats. The FIRST step that the homeowner should take after installation of all relevant cabling and hardware is to change the default passwords on new network devices.

Most modern routers come with default usernames and passwords that are widely known to potential attackers. If these defaults are not changed, it could make it easier for external attackers to gain unauthorized access to the network. Changing the passwords on new network devices is a simple but effective way to improve the security posture of the network.

---

### **Question: 538**

---

A technician is troubleshooting a PC that has been performing poorly. Looking at the Task Manager, the technician sees that CPU and memory resources seem fine, but disk throughput is at 100%.

Which of the following types of malware is the system MOST likely infected with?

- A . Keylogger
- B . Rootkit
- C . Ransomware
- D . Trojan

---

**Answer: C**

---

Explanation:

Ransomware is a type of malware that encrypts the files on the victim's computer and demands a ransom for their decryption. Ransomware can cause high disk throughput by encrypting large amounts of data in a short time.

---

### **Question: 539**

---

A neighbor successfully connected to a user's Wi-Fi network. Which of the following should the user do after changing the network configuration to prevent the neighbor from being able to connect again?

- A . Disable the SSID broadcast.
- B . Disable encryption settings.
- C . Disable DHCP reservations.
- D . Disable logging.

---

**Answer: A**

---

Explanation:

A) Disable the SSID broadcast1: The SSID broadcast is a feature that allows a Wi-Fi network to be visible to nearby devices. Disabling the SSID broadcast can make the network harder to find by unauthorized users, but it does not prevent them from accessing it if they know the network name and password.

---

### Question: 540

---

A technician is setting up a conference room computer with a script that boots the application on login. Which of the following would the technician use to accomplish this task? (Select TWO).

- A . File Explorer
- B . Startup Folder
- C . System Information
- D . Programs and Features
- E . Task Scheduler
- F . Device Manager

---

Answer: B, E

---

Explanation:

B) Startup Folder1: The Startup folder is a special folder that contains shortcuts to programs or scripts that will run automatically when a user logs on. The technician can create a shortcut to the script and place it in the Startup folder for the conference room computer or for all users.

E) Task Scheduler23: The Task Scheduler is a tool that allows you to create tasks that run at specified times or events. The technician can create a task that runs the script at logon for the conference room computer or for all users.

---

### Question: 541

---

A desktop engineer is deploying a master image. Which of the following should the desktop engineer consider when building the master image? (Select TWO).

- A . Device drivers
- B . Keyboard backlight settings
- C . Installed application license keys
- D . Display orientation
- E . Target device power supply
- F . Disabling express charging

---

Answer: A, C

---

Explanation:

A) Device drivers23: Device drivers are software components that enable the operating system to communicate with hardware devices. Different devices may require different drivers, so the desktop engineer should include the appropriate drivers in the master image or configure the deployment process to install them automatically.

C) Installed application license keys2: Installed application license keys are codes that activate or authenticate software applications. Some applications may require license keys to be entered during installation or after deployment. The desktop engineer should include the license keys in the master image or configure the deployment process to apply them automatically.

---

### Question: 542

---

A technician is troubleshooting boot times for a user. The technician attempts to use MSConfig to see which programs are starting with the OS but receives a message that it can no longer be used to view startup items. Which of the following programs can the technician use to view startup items?

- A . msinfo32
- B . perfmon
- C . regedit
- D . taskmgr

---

**Answer: D**

---

Explanation:

When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view startup items on a Windows system, but it may not always be available or functional.

In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task Manager (taskmgr), which can also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:

Open Task Manager by pressing Ctrl+Shift+Esc.

Click the 'Startup' tab.

The list of programs that run at startup will be displayed.

---

### Question: 543

---

A BSOD appears on a user's workstation monitor. The user immediately presses the power button to shut down the PC, hoping to repair the issue. The user then restarts the PC, and the BSOD reappears, so the user contacts the help desk. Which of the following should the technician use to determine the cause?

- A . Stop code
- B . Event Viewer
- C . Services

---

**Answer: A**

---

Explanation:

When a Blue Screen of Death (BSOD) appears on a Windows workstation, it indicates that there is a serious problem with the operating system. The stop code displayed on the BSOD can provide valuable information to help determine the cause of the issue. The stop code is a specific error code that is associated with the BSOD, and it can help identify the root cause of the problem.

In this scenario, the user has encountered a BSOD and has restarted the PC, only to see the BSOD reappear. This suggests that the problem is persistent and requires further investigation. By analyzing the stop code displayed on the BSOD, a technician can begin to identify the underlying issue and take appropriate actions to resolve it.

---

#### **Question: 544**

---

Which of the following editions of Windows 10 requires reactivation every 180 days?

- A . Enterprise
- B . Pro for Workstation
- C . Home
- D . Pro

---

**Answer: A**

---

Explanation:

Windows 10 Enterprise is an edition of Windows 10 that is designed for large organizations that need advanced security and management features. Windows 10 Enterprise can be activated using different methods, such as Multiple Activation Key (MAK), Active Directory-based Activation (ADBA), or Key Management Service (KMS). KMS is a method of activation that uses a local server to activate multiple devices on a network. KMS activations are valid for 180 days and need to be renewed periodically by connecting to the KMS server. If a device does not renew its activation within 180 days, it will enter a grace period of 30 days, after which it will display a warning message and lose some functionality until it is reactivated. The other editions of Windows 10 do not require reactivation every 180 days. Windows 10 Pro for Workstation is an edition of Windows 10 that is designed for high-performance devices that need advanced features such as ReFS file system, persistent memory, and faster file sharing. Windows 10 Pro for Workstation can be activated using a digital license or a product key. Windows 10 Home is an edition of Windows 10 that is designed for personal or home use. Windows 10 Home can be activated using a digital license or a product key. Windows 10 Pro is an edition of Windows 10 that is designed for business or professional use. Windows 10 Pro can be activated using a digital license or a product key. None of these editions require reactivation every 180 days unless there are significant hardware changes or other issues that affect the activation status.

---

#### **Question: 545**

---

A technician receives a call from a user who is unable to open Outlook. The user states that Outlook worked fine yesterday, but the computer may have restarted sometime overnight. Which of the following is the MOST likely reason Outlook has stopped functioning?

- A . Spam filter installation
- B . Invalid registry settings
- C . Malware infection
- D . Operating system update

---

**Answer: D**

---

Explanation:

Operating system updates can sometimes cause compatibility issues with some applications, such as Outlook, that may prevent them from opening or working properly. This can happen if the update changes some system files or settings that Outlook relies on, or if the update conflicts with some Outlook add-ins or extensions. To fix this, the technician can try some of these troubleshooting steps:

[Start Outlook in safe mode and disable add-ins. Safe mode is a way of starting Outlook without any add-ins or extensions that may interfere with its functionality. To start Outlook in safe mode, press and hold the Ctrl key while clicking on the Outlook icon. You should see a message asking if you want to start Outlook in safe mode. Click Yes. If Outlook works fine in safe mode, it means one of the add-ins is causing the problem. To disable add-ins, go to File > Options > Add-ins. In the Manage drop-down list, select COM Add-ins and click Go. Uncheck any add-ins that you don't need and click OK. Restart Outlook normally and check if the issue is resolved4.](#)

[Create a new Outlook profile. A profile is a set of settings and information that Outlook uses to manage your email accounts and data. Sometimes, a profile can get corrupted or damaged and cause Outlook to malfunction. To create a new profile, go to Control Panel > Mail > Show Profiles. Click Add and follow the instructions to set up a new profile with your email account. Make sure to select the option to use the new profile as the default one. Restart Outlook and check if the issue is resolved5.](#)

Repair your Outlook data files. Data files are files that store your email messages, contacts, calendar events, and other items on your computer. Sometimes, data files can get corrupted or damaged and cause Outlook to malfunction. To repair your data files, you can use a tool called scanpst.exe, which is located in the same folder where Outlook is installed (usually C:\Program Files\Microsoft Office\root\Office16). To use scanpst.exe, close Outlook and locate the tool in the folder. Double-click on it and browse to the location of your data file (usually C:\Users\username\AppData\Local\Microsoft\Outlook). Select the file and click Start to begin the scanning and repairing process. When it's done, restart Outlook and check if the issue is resolved.

Run the /resetnavpane command. The navigation pane is the panel on the left side of Outlook that shows your folders and accounts. Sometimes, the navigation pane can get corrupted or damaged and cause Outlook to malfunction. To reset the navigation pane, press Windows key + R to open the Run dialog box, or open the Command Prompt. Type outlook.exe /resetnavpane and hit Enter. This will clear and regenerate the navigation pane settings for Outlook. Restart Outlook and check if the issue is resolved.

---

### Question: 546

---

A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore

times but asks the technician to retain more versions when possible. Which of the following backup methods should the technician MOST likely implement?

- A . Full
- B . Mirror
- C . Incremental
- D . Differential

---

**Answer: C**

---

Explanation:

Incremental backup is a backup method that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup can save storage space and bandwidth, as it does not copy the same files over and over again. Incremental backup can also retain more versions of backups, as it only stores the changes made to the files. However, incremental backup can have longer restore times, as it requires restoring the last full backup and all the subsequent incremental backups in order to recover the data. The law firm is not concerned about restore times but asks the technician to retain more versions when possible, so incremental backup would be a suitable choice for them.

---

### **Question: 547**

---

A user needs assistance installing software on a Windows PC but will not be in the office. Which of the following solutions would a technician MOST likely use to assist the user without having to install additional software?

- A . VPN
- B . MSRA
- C . SSH
- D . RDP

---

**Answer: B**

---

Explanation:

MSRA stands for Microsoft Remote Assistance, and it is a feature that allows a technician to remotely view and control another user's Windows PC with their permission. MSRA is built-in to Windows and does not require any additional software installation. To use MSRA, the technician and the user need to follow these steps:

On the user's PC, type msra in the search box on the taskbar and select Invite someone to connect to your PC and help you, or offer to help someone else.

Select Save this invitation as a file and choose a location to save the file. This file contains a password that the technician will need to connect to the user's PC.

Send the file and the password to the technician via email or another secure method.

On the technician's PC, type msra in the search box on the taskbar and select Help someone who has invited you.

Select Use an invitation file and browse to the location where the file from the user is saved. Enter the password when prompted.

The user will see a message asking if they want to allow the technician to connect to their PC. The user should select Yes.

The technician will see the user's desktop and can request control of their PC by clicking Request control on the top bar. The user should allow this request by clicking Yes.

The technician can now view and control the user's PC and assist them with installing software.

---

### Question: 548

---

A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:

crypt32.dll is missing not found

Which of the following should the technician attempt FIRST?

- A . Rebuild Windows profiles.
- B . Reimage the workstation
- C . Roll back updates
- D . Perform a system file check

---

**Answer: D**

---

Explanation:

If this file is missing or corrupted, it can cause application crashes or errors when trying to open websites in a browser. To fix this, the technician can perform a system file check, which is a utility that scans and repairs corrupted or missing system files. To perform a system file check, the technician can follow these steps:

Open the Command Prompt as an administrator. To do this, type cmd in the search box on the taskbar, right-click on Command Prompt, and select Run as administrator.

In the Command Prompt window, type sfc /scannow and hit Enter. This will start the scanning and repairing process, which may take some time.

Wait for the process to complete. If any problems are found and fixed, you will see a message saying Windows Resource Protection found corrupt files and successfully repaired them. If no problems are found, you will see a message saying Windows Resource Protection did not find any integrity violations.

Restart your computer and check if the issue is resolved.

---

### Question: 549

---

A technician needs to provide recommendations about how to upgrade backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. Which of the following should the technician recommend implementing?

- A . High availability
- B . Regionally diverse backups
- C . On-site backups
- D . Incremental backups

---

**Answer: B**

---

Explanation:

Regionally diverse backups are backups that are stored in different geographic locations, preferably far away from the primary site.1. This way, if a disaster such as a hurricane or a power outage affects one location, the backups in another location will still be available and accessible2. Regionally diverse backups can help ensure business continuity and data recovery in case of a disaster3. The other options are not the best backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. High availability is a feature that allows a system to remain operational and accessible even if one or more components fail, but it does not protect against data loss or corruption4. On-site backups are backups that are stored in the same location as the primary site, which means they are vulnerable to the same disasters that can affect the primary site. Incremental backups are backups that only store the changes made since the last backup, which means they require less storage space and bandwidth, but they also depend on previous backups to restore data and may not be sufficient for disaster recovery.

---

### **Question: 550**

---

A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

- A . Delete the application's cache.
- B . Check for application updates.
- C . Roll back the OS update.
- D . Uninstall and reinstall the application.

---

**Answer: B**

---

Explanation:

Sometimes, an OS update can cause compatibility issues with some applications that are not optimized for the new version of the OS. To fix this, the user should check if there are any updates available for the application that can resolve the issue. The user can check for application updates by following these steps:

On an Android device, open the Google Play Store app and tap on the menu icon in the top left corner. Then tap on My apps & games and look for any updates available for the application. If there is an update, tap on Update to install it.

On an iOS device, open the App Store app and tap on the Updates tab at the bottom. Then look for any updates available for the application. If there is an update, tap on Update to install it.

---

### **Question: 551**

---

Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed FIRST to prevent further damage to the host and other systems?

- A . Power off the machine.
- B . Run a full antivirus scan.
- C . Remove the LAN card.
- D . Install a different endpoint solution.

---

**Answer: A**

---

Explanation:

Ransomware is a type of malware that encrypts the files on a system and demands a ransom for their decryption1. Ransomware can also spread to other systems on the network or exfiltrate sensitive data to the attackers2. Therefore, it is important to isolate the infected machine as soon as possible to contain the infection and prevent further damage3. Powering off the machine is a quick and effective way of disconnecting it from the network and stopping any malicious processes running on it12. The other options are not directly related to preventing ransomware damage or may not be effective. Running a full antivirus scan may not be able to detect or remove the ransomware, especially if it is a new or unknown variant1. Removing the LAN card may disconnect the machine from the network, but it may not stop any malicious processes running on it or any data encryption or exfiltration that has already occurred2. Installing a different endpoint solution may not be possible or helpful if the system is already infected and locked by ransomware1.

Topic 3, Exam Pool C

---

### **Question: 552**

---

A mobile phone user has downloaded a new payment application that allows payments to be made with a mobile device. The user attempts to use the device at a payment terminal but is unable to do so successfully. The user contacts a help desk technician to report the issue. Which of the following should the technician confirm NEXT as part of the troubleshooting process?

- A . If airplane mode is enabled
- B . If Bluetooth is disabled
- C . If NFC is enabled
- D . If WiFi is enabled
- E . If location services are disabled

---

**Answer: C**

---

Explanation:

NFC stands for Near Field Communication, and it is a wireless technology that allows your phone to act as a contactless payment device, among other things<sup>2</sup>. Payment applications that allow payments to be made with a mobile device usually rely on NFC to communicate with the payment terminal<sup>1</sup>. Therefore, if NFC is disabled on the phone, the payment will not work. To enable NFC on an Android phone, you need to follow these steps<sup>3</sup>:

On your Android device, open the Settings app.

Select Connected devices.

Tap on Connection preferences.

You should see the NFC option. Toggle it on.

The other options are not directly related to using a payment application with a mobile device. Airplane mode is a setting that disables all wireless communication on the phone, including NFC<sup>4</sup>, but it also affects calls, texts, and internet access. Bluetooth is a wireless technology that allows you to connect your phone with other devices such as headphones or speakers, but it is not used for contactless payments. Wi-Fi is a wireless technology that allows you to access the internet or a local network, but it is also not used for contactless payments. Location services are a feature that allows your phone to determine your geographic location using GPS or other methods, but they are not required for contactless payments.

---

## Question: 553

---

A technician needs to manually set an IP address on a computer that is running macOS. Which of the following commands should the technician use?

- A . ipconfig
- B . ifconfig
- C . arpa
- D . ping

---

**Answer: B**

---

Explanation:

ifconfig is a command-line utility that allows you to configure network interfaces on macOS and other Unix-like systems<sup>1</sup>. To set an IP address using ifconfig, you need to know the name of the network interface you want to configure (such as en0 or en1), and the IP address you want to assign (such as 192.168.0.150). You also need to use sudo to run the command with administrative privileges<sup>2</sup>. The syntax of the command is:

sudo ifconfig interface address

For example, to set the IP address of en1 to 192.168.0.150, you would type:

sudo ifconfig en1 192.168.0.150

You may also need to specify other parameters such as subnet mask, gateway, or DNS servers, depending on your network configuration<sup>3</sup>. The other commands are not directly related to setting an IP address on macOS. ipconfig is a similar command for Windows systems<sup>4</sup>, arpa is a domain name used for reverse DNS lookup, and ping is a command for testing network connectivity.

---

## **Question: 554**

---

A technician is troubleshooting an issue that requires a user profile to be rebuilt. The technician is unable to locate Local Users and Groups in the Mtv1C console. Which of the following is the NEXT step the technician should take to resolve the issue?

- A . Run the antivirus scan.
- B . Add the required snap-in.
- C . Restore the system backup
- D . use the administrator console.

---

**Answer: B**

---

Explanation:

[Local Users and Groups is a Microsoft Management Console \(MMC\) snap-in that allows you to manage user accounts or groups on your computer1.If you cannot find it in the MMC console, you can add it manually by following these steps2:](#)

Press Windows key + R to open the Run dialog box, or open the Command Prompt.

Type mmc and hit Enter. This will open a blank MMC console.

Click File and then Add/Remove Snap-in.

In the Add or Remove Snap-ins window, select Local Users and Groups from the Available snap-ins list, and click Add.

In the Select Computer window, choose Local computer or Another computer, depending on which computer you want to manage, and click Finish.

Click OK to close the Add or Remove Snap-ins window. You should now see Local Users and Groups in the MMC console.

---

## **Question: 555**

---

A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

- A . Signed system images
- B . Antivirus
- C . SSO
- D . MDM

---

**Answer: D**

---

Explanation:

MDM stands for Mobile Device Management, and it is a way of remotely managing and securing mobile devices that are used for work purposes1.MDM can enforce policies and restrictions on the devices, such as preventing users from installing unauthorized apps, modifying system settings, or accessing root privileges2.MDM can also monitor device status, wipe data, lock devices, or locate lost or stolen devices1.

---

### **Question: 556**

---

A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the login issue?

- A . Expired certificate
- B . OS update failure
- C . Service not started
- D . Application crash
- E . Profile rebuild needed

---

**Answer: A**

---

Explanation:

EAP-TLS is a method of authentication that uses certificates to establish a secure tunnel between the client and the server3.The certificates have a validity period and must be renewed before they expire1.If the user has been on an extended leave and has not logged in to the computer in several months, it is possible that the certificate on the client or the server has expired and needs to be renewed2.The other options are not directly related to EAP-TLS authentication or 802.1X network access.

---

### **Question: 557**

---

A team of support agents will be using their workstations to store credit card dat

a. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).

- A . Encryption
- B . Antivirus
- C . AutoRun
- D . Guest accounts
- E . Default passwords
- F . Backups

---

**Answer: A, F**

---

Explanation:

Encryption is a way of protecting cardholder data by transforming it into an unreadable format that can only be decrypted with a secret key1. Backups are a way of ensuring that cardholder data is not lost or corrupted in case of a disaster or system failure2. Both encryption and backups are part of the PCI DSS requirements that apply to any entity that stores, processes, or transmits cardholder data1. The other options are not directly related to credit card data security or compliance.

---

### Question: 558

---

A technician is troubleshooting a computer with a suspected short in the power supply. Which of the following is the FIRST step the technician should take?

- A . Put on an ESD strap
- B . Disconnect the power before servicing the PC.
- C . Place the PC on a grounded workbench.
- D . Place components on an ESD mat.

---

**Answer: B**

---

Explanation:

The first step a technician should take when troubleshooting a computer with a suspected short in the power supply isB. Disconnect the power before servicing the PC. This is to prevent any electrical shock or damage to the components.A power supply can be dangerous even when unplugged, as capacitors can maintain a line voltage charge for a long time1. Therefore, it is important to disconnect the power cord and press the power button to discharge any residual power before opening the case2. The other steps are also important for safety and proper diagnosis, but they should be done after disconnecting the power.

---

### Question: 559

---

A macOS user needs to create another virtual desktop space. Which of the following applications will allow the user to accomplish this task?

- A . Dock
- B . Spotlight
- C . Mission Control
- D . Launchpad

---

**Answer: C**

---

Explanation:

application that will allow a macOS user to create another virtual desktop space isMission Control Mission Control lets you create additional desktops, called spaces, to organize the windows of your apps. You can create a space by entering Mission Control and clicking the Add button in the Spaces bar1. You can also assign apps to specific spaces and move between them easily1.

## **Question: 560**

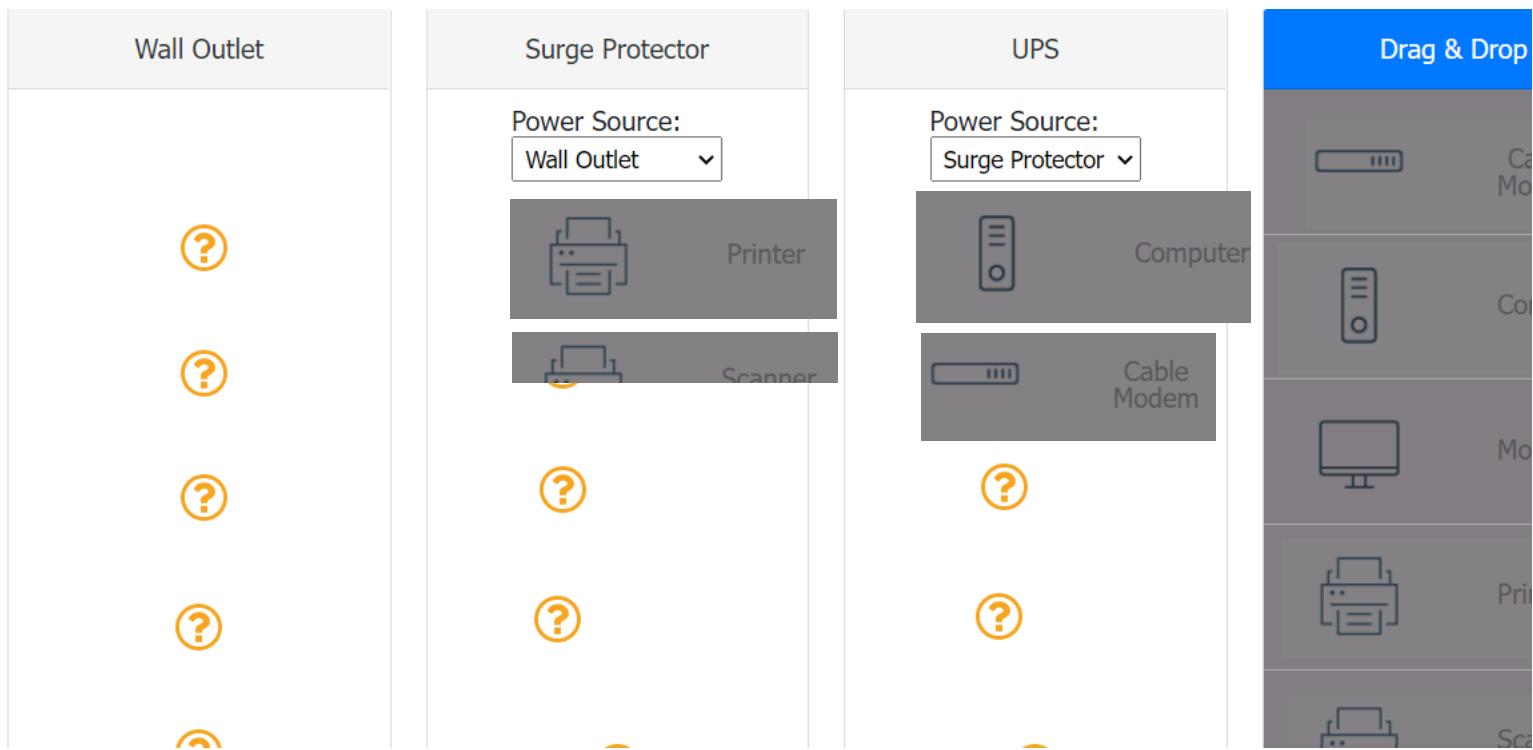
A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.

Wall Outlet	Surge Protector	UPS	Drag & Drop
?	Power Source: Wall Outlet	Power Source: Surge Protector	Cable Modem
?	?	?	Computer
?	?	?	Monitor
?	?	?	Printer
?	-	-	Scanner

---

**Answer:**

---



### **Question: 561**

A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

- A . resmon\_exe
- B . dfrgui\_exe
- C . msinfo32exe
- D . msconfig\_exe

---

**Answer: A**

---

Explanation:

If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O. Resource Monitor provides detailed information about the system's resource usage, including disk I/O. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action.

### **Question: 562**

A new spam gateway was recently deployed at a small business. However, users still occasionally receive spam. The management team is concerned that users will open the messages and potentially

infect the network systems. Which of the following is the MOST effective method for dealing with this issue?

- A . Adjusting the spam gateway
- B . Updating firmware for the spam appliance

- C . Adjusting AV settings
- D . Providing user training

---

**Answer: D**

---

Explanation:

The most effective method for dealing with spam messages in a small business is to provide user training1.Users should be trained to recognize spam messages and avoid opening them1.They should also be trained to report spam messages to the IT department so that appropriate action can be taken1.In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources1.By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems1.

---

### **Question: 563**

---

After a company installed a new SOHO router customers were unable to access the company-hosted public website. Which of the following will MOST likely allow customers to access the website?

- A . Port forwarding
- B . Firmware updates
- C . IP filtering
- D . Content filtering

---

**Answer: B**

---

Explanation:

If customers are unable to access the company-hosted public website after installing a new SOHO router, the company should check for firmware updates1.Firmware updates can fix bugs and compatibility issues that may be preventing customers from accessing the website1.The company should also ensure that the router is properly configured to allow traffic to the website1.If the router is blocking traffic to the website, the company should configure the router to allow traffic to the website1.

---

### **Question: 564**

---

A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

- A . Drilling
- B . Degaussing
- C . Low-level formatting
- D . Erasing/wiping

---

**Answer: D**

---

Explanation:

Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

---

### Question: 565

---

A user is unable to access a website, which is widely used across the organization, and receives the following error message:

The security certificate presented by this website has expired or is not yet valid.

The technician confirms the website works when accessing it from another computer but not from the user's computer. Which of the following should the technician perform NEXT to troubleshoot the issue?

- A . Reboot the computer.
- B . Reinstall the OS.
- C . Configure a static IP.
- D . Check the computer's date and time.

---

Answer: D

---

Explanation:

The error message indicates that the security certificate presented by the website has either expired or is not yet valid. This can happen if the computer's clock has the wrong date or time, as SSL/TLS certificates have a specific validity period. If the clock is off by too much, it may cause the certificate to fail to validate. Therefore, the technician should check the computer's date and time and ensure that they are correct.

---

### Question: 566

---

Following a recent power outage, several computers have been receiving errors when booting. The technician suspects file corruption has occurred. Which of the following steps should the technician try FIRST to correct the issue?

- A . Rebuild the Windows profiles.
- B . Restore the computers from backup.
- C . Reimage the computers.
- D . Run the System File Checker.

---

Answer: D

---

Explanation:

[The technician should run the System File Checker \(SFC\) first to correct file corruption errors on computers after a power outage. SFC is a command-line utility that scans for and repairs corrupted system files. It can be run from the command prompt or from the Windows Recovery Environment. Rebuilding the Windows profiles, restoring the computers from backup, and reimaging the computers are more drastic measures that should be taken only if SFC fails to correct the issue1](#)

---

### **Question: 567**

---

The web browsing speed on a customer's mobile phone slows down every few weeks and then returns to normal after three or four days. Restarting the device does not usually restore performance. Which of the following should a technician check FIRST to troubleshoot this issue?

- A . Data usage limits
- B . Wi-Fi connection speed
- C . Status of airplane mode
- D . System uptime

---

**Answer: B**

---

Explanation:

The technician should check the Wi-Fi connection speed first to troubleshoot this issue. Slow web browsing speed on a mobile phone can be caused by a slow Wi-Fi connection. The technician should check the Wi-Fi connection speed to ensure that it is fast enough to support web browsing. If the Wi-Fi connection speed is slow, the technician should troubleshoot the Wi-Fi network to identify and resolve the issue.

---

### **Question: 568**

---

A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

- A . UEFI password
- B . Secure boot
- C . Account lockout
- D . Restricted user permissions

---

**Answer: B**

---

Explanation:

A technician setting up a new laptop must ensure that users cannot install virtual machines as the company's security policy states. One way to prevent users from enabling virtual technology is by implementing Secure Boot. Secure Boot is a feature of UEFI firmware that ensures the system only boots using firmware that is trusted by the manufacturer. It verifies the signature of all bootloaders, operating systems, and drivers before running them, preventing any

Unauthorized modifications to the boot process. This will help prevent users from installing virtual machines on the laptop without authorization.

---

### Question: 569

---

A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on

multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?

- A . Use the application only on the home laptop because it contains the initial license.
- B . Use the application at home and contact the vendor regarding a corporate license.
- C . Use the application on any computer since the user has a license.
- D . Use the application only on corporate computers.

---

**Answer: B**

---

Explanation:

Use the application at home and contact the vendor regarding a corporate license. The user should use the application only on the home laptop because it contains the initial license. The user should contact the vendor regarding a corporate license if they want to use the application on multiple computers on the corporate network1

---

### Question: 570

---

A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

- A . Surge suppressor
- B . Battery backup
- C . CMOS battery
- D . Generator backup

---

**Answer: B**

---

Explanation:

A battery backup, also known as an uninterruptible power supply (UPS), is a device that provides backup power during a power outage. When the power goes out, the battery backup provides a short amount of time (usually a few minutes up to an hour, depending on the capacity of the device) to save any work and safely shut down the equipment.

---

## **Question: 571**

---

Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell. Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

- A . Restore the device to factory settings.
- B . Uninstall the unapproved application.
- C . Disable the ability to install applications from unknown sources.
- D . Ensure the device is connected to the corporate WiFi network.

---

**Answer: B**

---

Explanation:

The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario1

---

## **Question: 572**

---

In which of the following scenarios would remote wipe capabilities MOST likely be used? (Select TWO).

- A . A new IT policy requires users to set up a lock screen PIN.
- B . A user is overseas and wants to use a compatible international SIM Card.
- C . A user left the phone at home and wants to prevent children from gaining access to the phone.
- D . A user traded in the company phone for a cell carrier upgrade by mistake.
- E . A user cannot locate the phone after attending a play at a theater.
- F . A user forgot the phone in a taxi, and the driver called the company to return the device.

---

**Answer: E, F**

---

Explanation:

Remote wipe capabilities are used to erase all data on a mobile device remotely. This can be useful in situations where a device is lost or stolen, or when sensitive data needs to be removed from a device. Remote wipe capabilities are most likely to be used in the following scenarios:

E) A user cannot locate the phone after attending a play at a theater. F.A user forgot the phone in a taxi, and the driver called the company to return the device1

In scenario E, remote wipe capabilities would be used to prevent unauthorized access to the device and to protect sensitive data. In scenario F, remote wipe capabilities would be used to erase all data on the device before it is returned to the user.

---

### Question: 573

---

A network administrator is deploying a client certificate to be used for Wi-Fi access for all devices in an organization. The certificate will be used in conjunction with the user's existing username and password. Which of the following BEST describes the security benefits realized after this deployment?

- A . Multifactor authentication will be forced for Wi-Fi.
- B . All Wi-Fi traffic will be encrypted in transit.
- C . Eavesdropping attempts will be prevented.
- D . Rogue access points will not connect.

---

**Answer: B**

---

Explanation:

The security benefits realized after deploying a client certificate to be used for Wi-Fi access for all devices in an organization are that all Wi-Fi traffic will be encrypted in transit. This means that any data transmitted over the Wi-Fi network will be protected from eavesdropping attempts. Rogue access points will not connect to the network because they will not have the client certificate. However, multifactor authentication will not be forced for Wi-Fi because the client certificate is being used in conjunction with the user's existing username and password12

---

### Question: 574

---

Which of the following change management documents includes how to uninstall a patch?

- A . Purpose of change
- B . Rollback plan
- C . Scope of change
- D . Risk analysis

---

**Answer: B**

---

Explanation:

The change management document that includes how to uninstall a patch is called the "rollback plan". The rollback plan is a document that outlines the steps that should be taken to undo a change that has been made to a system. In the case of a patch, the rollback plan would include instructions on how to uninstall the patch if it causes problems or conflicts with other software12

---

## **Question: 575**

---

A user connected a laptop to a wireless network and was tricked into providing login credentials for a website. Which of the following threats was used to carry out the attack?

- A . Zero day
- B . Vishing
- C . DDoS
- D . Evil twin

---

**Answer: B**

---

Explanation:

Vishing, also known as voice phishing, is a type of social engineering attack where the attacker tricks the victim into divulging sensitive information over the phone. In this case, the attacker tricked the user into providing login credentials for a website.

---

## **Question: 576**

---

A user's system is infected with malware. A technician updates the anti-malware software and runs a scan that removes the malware. After the user reboots the system, it once again becomes infected with malware. Which of the following will MOST likely help to permanently remove the malware?

- A . Enabling System Restore
- B . Educating the user
- C . Booting into safe mode
- D . Scheduling a scan

---

**Answer: B**

---

Explanation:

Although updating the anti-malware software and running scans are important steps in removing malware, they may not be sufficient to permanently remove the malware if the user keeps engaging in behaviors that leave the system vulnerable, such as downloading unknown files or visiting malicious websites. Therefore, educating the user on safe computing practices is the best way to prevent future infections and permanently remove the malware.

Enabling System Restore, Booting into safe mode, and scheduling a scan are not the most efficient ways to permanently remove the malware. Enabling System Restore and Booting into safe mode may help in some cases, but they may not be sufficient to permanently remove the malware. Scheduling a scan is also important for detecting and removing malware, but it may not be sufficient to prevent future infections.

---

## **Question: 577**

---

A technician has an external SSD. The technician needs to read and write to an external SSD on both Macs and Windows PCs. Which of the following filesystems is supported by both OS types?

- A . NTFS
- B . APFS
- C . ext4
- D . exFAT

---

**Answer: D**

---

Explanation:

The filesystem that is supported by both Macs and Windows PCs is D. exFAT. exFAT is a file system that is designed to be used on flash drives like USB sticks and SD cards. It is supported by both Macs and Windows PCs, and it can handle large files and volumes

<https://www.diskpart.com/articles/file-system-for-mac-and-windows-0310.html>

---

## **Question: 578**

---

Which of the following is the STRONGEST wireless configuration?

- A . WPS
- B . WPA3
- C . WEP
- D . WMN

---

**Answer: B**

---

Explanation:

The strongest wireless configuration is B. WPA3. WPA3 is the most up-to-date wireless encryption protocol and is the most secure choice. It replaces PSK with SAE, a more secure way to do the initial key exchange. At the same time, the session key size of WPA3 increases to 128-bit in WPA3-Personal mode and 192-bit in WPA3-Enterprise, which makes the password harder to crack than the previous Wi-Fi security standards

<https://www.makeuseof.com/tag/wep-wpa-wpa2-wpa3-explained/>

---

## **Question: 579**

---

Each time a user tries to go to the selected web search provider, a different website opens. Which of the following should the technician check FIRST?

- A . System time
- B . IP address
- C . DNS servers
- D . Windows updates

---

**Answer: C**

---

Explanation:

When a user experiences unexpected or erratic behavior while browsing the internet, it could be caused by the DNS servers. DNS translates human-readable domain names (like google.com) into IP addresses, which computers can use to communicate with web servers. If the DNS servers are not functioning correctly or have been compromised, it can result in the browser being redirected to unintended websites.

---

### **Question: 580**

---

A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

- A . Escalate the ticket to Tier 2.
- B . Run a virus scan.
- C . Utilize a Windows restore point.
- D . Reimage the computer.

---

**Answer: B**

---

Explanation:

[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\).pdf](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0).pdf)

When a user reports that their workstation is behaving strangely after opening a suspicious email, the first step a technician should take is to run a virus scan on the computer. This is because opening a suspicious email is a common way for viruses and malware to infect a computer. Running a virus scan can help identify and remove any infections that may be causing the computer to behave strangely.

---

### **Question: 581**

---

An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

- A . Risk analysis
- B . Sandbox testing
- C . End user acceptance
- D . Lessons learned

---

**Answer: A**

---

Explanation:

[A risk analysis must be completed before a change request for an upcoming server deployment can be approved1](#)

Risk analysis is an important step in the change management process because it helps identify and mitigate potential risks before changes are implemented. Once the risks have been analyzed and the appropriate measures have been taken to minimize them, the change can be approved and implemented.

---

### **Question: 582**

---

A junior administrator is responsible for deploying software to a large group of computers in an organization. The administrator finds a script on a popular coding website to automate this distribution but does not understand the scripting language. Which of the following BEST describes the risks in running this script?

- A . The instructions from the software company are not being followed.
- B . Security controls will treat automated deployments as malware.
- C . The deployment script is performing unknown actions.
- D . Copying scripts off the internet is considered plagiarism.

---

**Answer: C**

---

Explanation:

[The risks in running this script are that the deployment script is performing unknown actions. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data1.](#)

---

### **Question: 583**

---

A user is attempting to make a purchase at a store using a phone. The user places the phone on the payment pad, but the device does not recognize the phone. The user attempts to restart the phone but still has the same results. Which of the following should the user do to resolve the issue?

- A . Turn off airplane mode while at the register.
- B . Verify that NFC is enabled.
- C . Connect to the store's Wi-Fi network.
- D . Enable Bluetooth on the phone.

---

**Answer: B**

---

Explanation:

The user should verify that NFC is enabled on their phone. NFC is a technology that allows two devices to communicate with each other when they are in close proximity2.

NFC (Near Field Communication) technology allows a phone to wirelessly communicate with a payment terminal or other compatible device. In order to use NFC to make a payment or transfer information, the feature must be enabled on the phone. Therefore, the user should verify that NFC is enabled on their phone before attempting to make a payment with it. The other options, such as turning off airplane mode, connecting to Wi-Fi, or enabling Bluetooth, do not pertain to the NFC feature and are unlikely to resolve the issue. This information is covered in the Comptia A+ Core2 documents/guide under the Mobile Devices section.

---

### **Question: 584**

---

A laptop user is visually impaired and requires a different cursor color. Which of the following OS utilities is used to change the color of the cursor?

- A . Keyboard
- B . Touch pad
- C . Ease of Access Center
- D . Display settings

---

**Answer: C**

---

Explanation:

The OS utility used to change the color of the cursor in Windows is Ease of Access Center12

The user can change the cursor color by opening the Settings app, selecting Accessibility in the left sidebar, selecting Mouse pointer and touch under Vision, and choosing one of the cursor options. The user can select Custom to pick a color and use the Size slider to make the cursor larger or smaller12

The Ease of Access Center in the Windows OS provides accessibility options for users with disabilities or impairments. One of these options allows the user to change the color and size of the cursor, making it more visible and easier to locate on the screen. The Keyboard and Touchpad settings do not offer the option to change cursor color, and Display Settings are used to adjust the resolution and other properties of the display. Therefore, C is the best answer. This information is covered in the Comptia A+ Core2 documents/guide under the Accessibility section.

---

### **Question: 585**

---

A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has asked for this setting to be changed. Which of the following tools would the technician MOST likely use to safely make this change?

- A . Registry Editor
- B . Task Manager
- C . Event Viewer
- D . Local Users and Groups

Explanation:

[The technician would most likely use the Task Manager tool to safely make this change](#)<sup>12</sup>

[The Task Manager tool can be used to disable applications from starting automatically on Windows 10](#)

The tool that a technician would most likely use to stop an application from automatically starting when a user logs in to a Windows 10 system is the Task Manager. The Task Manager can be used to view and manage processes, including those that are set to automatically start when a user logs in to the system.

---

### **Question: 586**

---

Which of the following is MOST likely contained in an EULA?

- A . Chain of custody
- B . Backup of software code
- C . Personally identifiable information
- D . Restrictions of use

Explanation:

[An EULA \(End-User License Agreement\) is a legally binding contract between a software supplier and a customer or end-user, generally made available to the customer via a retailer acting as an intermediary. A EULA specifies in detail the rights and restrictions which apply to the use of the software. Some of the main terms included in an EULA are the terms and scope of the license, any licensing fees, warranties and disclaimers, limitation of liability, revocation or termination of the license, and intellectual property information and restrictions on using the license \(e.g. modification and copying\)](#)<sup>1</sup>

<https://www.termsfeed.com/blog/eula-vs-terms-conditions/>

---

### **Question: 587**

---

A user is setting up a computer for the first time and would like to create a secondary login with permissions that are different than the primary login. The secondary login will need to be protected from certain content such as games and websites. Which of the following Windows settings should the user utilize to create the secondary login?

- A . Privacy
- B . Accounts
- C . Personalization
- D . Shared resources

---

**Answer: B**

---

Explanation:

To create a secondary login with different permissions in Windows 10, the user should utilize the Accounts setting. Here are the steps to create a new user account with different permissions:

Right-click the Windows Start menu button.

Select Control Panel.

Select User Accounts.

Select Manage another account.

Select Add a new user in PC settings.

[Use the Accounts dialog box to configure a new account.1](#)

---

**Question: 588**

---

A small business owner wants to install newly purchased software on all networked PCs. The network is not configured as a domain, and the owner wants to use the easiest method possible. Which of the following is the MOST deficient way for the owner to install the application?

- A . Use a network share to share the installation files.
- B . Save software to an external hard drive to install.
- C . Create an imaging USB for each PC.
- D . Install the software from the vendor's website

---

**Answer: B**

---

Explanation:

Saving software to an external hard drive and installing it on each individual PC is the most inefficient method for the small business owner. This method requires manual intervention on each PC, and there is a higher risk of error or inconsistencies between PCs. Additionally, if the software needs to be updated or reinstalled in the future, this process would need to be repeated on each PC.

---

**Question: 589**

---

A Microsoft Windows PC needs to be set up for a user at a large corporation. The user will need access to the corporate domain to access email and shared drives. Which of the following versions of Windows would a technician MOST likely deploy for the user?

- A . Windows Enterprise Edition
- B . Windows Professional Edition
- C . Windows Server Standard Edition
- D . Windows Home Edition

---

**Answer: B**

---

Explanation:

The Windows Professional Edition is the most likely version that a technician would deploy for a user at a target corporation. This version of Windows is designed for business use and provides the necessary features and capabilities that a user would need to access the corporate domain, such as email and shared drives.

---

### **Question: 590**

---

A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

- A . Enable multifactor authentication.
- B . Increase the failed log-in threshold.
- C . Remove complex password requirements.
- D . Implement a single sign-on with biometrics.

---

**Answer: A**

---

Explanation:

Multifactor authentication (MFA) is a security measure that requires users to provide multiple pieces of evidence when logging in to an account or system. This can include a combination of something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smartphone) and something the user is (e.g. biometrics such as a fingerprint or face scan). By enabling MFA, the systems administrator can ensure that users are required to provide multiple pieces of evidence when logging in, making it more difficult for unauthorized users to gain access to the system. This can help reduce the number of help desk tickets submitted due to forgotten passwords.

---

### **Question: 591**

---

A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

- A . Avoid distractions
- B . Deal appropriately with customer's confidential material .
- C . Adhere to user privacy policy
- D . Set and meet timelines

---

**Answer: A**

---

Explanation:

The technician's action of setting the phone to silent while troubleshooting the customer's PC is an example of avoiding distractions. By setting the phone to silent, the technician is ensuring that they are able to focus on the task at hand without any distractions that could potentially disrupt their workflow. This is an important practice when handling customer's confidential material, as it ensures that the technician is able to focus on the task and not be distracted by any external sources. Furthermore, it also adheres to user privacy policies, as the technician is not exposing any confidential information to any external sources.

---

**Question: 592**

---

An administrator has received approval for a change request for an upcoming server deployment. Which of the following steps should be completed NEXT?

- A . Perform a risk analysis.
- B . Implement the deployment.
- C . Verify end user acceptance
- D . Document the lessons learned.

---

**Answer: A**

---

Explanation:

Before making any changes to the system, it is important to assess the risks associated with the change and determine whether it is worth implementing. Risk analysis involves identifying potential risks, assessing their likelihood and impact, and determining what steps can be taken to mitigate them. It is important to perform this step before making any changes, as this allows the administrator to make an informed decision about whether or not the change should be implemented. Once the risks have been assessed and the administrator has decided to go ahead with the change, the next step is to implement the deployment.

---

**Question: 593**

---

A technician received a call stating that all files in a user's documents folder appear to be Changed, and each of the files now has a .look file extension. Which of the following actions is the FIRST step the technician should take?

- A . Run a live disk clone.
- B . Run a full antivirus scan.
- C . Use a batch file to rename the files.
- D . Disconnect the machine from the network

---

**Answer: D**

---

Explanation:

The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains: 1.2 Given a scenario, use appropriate resources to support users and 1.3 Explain the importance of security awareness.

---

### **Question: 594**

---

A systems administrator needs to reset a user's password because the user forgot it. The systems administrator creates the new password and wants to further protect the user's account. Which of the following should the systems administrator do?

- A . Require the user to change the password at the next log-in.
- B . Disallow the user from changing the password.
- C . Disable the account
- D . Choose a password that never expires.

---

**Answer: A**

---

Explanation:

This will ensure that the user is the only one who knows their password, and that the new password is secure.

The CompTIA A+ Core 2 220-1002 exam covers this topic in the domain 1.4 Given a scenario, use appropriate data destruction and disposal methods.

---

### **Question: 595**

---

A technician has verified that a user's computer has a virus, and the antivirus software is out of date. Which of the following steps should the technician take NEXT?

- A . Quarantine the computer.
- B . Use a previous restore point,
- C . Educate the end user about viruses
- D . Download the latest virus definitions

---

**Answer: D**

---

Explanation:

This will ensure that the antivirus software is up-to-date, and can detect any new viruses that may have been released since the last virus definition update.

The CompTIA A+ Core 2 220-1102 exam covers this topic in the following domains: 1.3 Explain the importance of security awareness and 2.2 Given a scenario, use secure data management and disaster recovery principles.

---

### Question: 596

---

An IT services company that supports a large government contract replaced the Ethernet cards on several hundred desktop machines to comply With regulatory requirements. Which of the following disposal methods for the non-compliant cards is the MOST environmentally friendly?

- A . incineration
- B . Resale
- C . Physical destruction
- D . Dumpster for recycling plastics

---

**Answer: D**

---

Explanation:

When disposing of non-compliant Ethernet cards, the most environmentally friendly option is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials. Additionally, recycling plastics helps to reduce the amount of toxic chemicals that can be released into the environment.

According to CompTIA A+ Core 2 documents, 'The most environmentally friendly disposal method for non-compliant Ethernet cards is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials.'

<https://sustainability.yale.edu/blog/how-sustainably-dispose-your-technological-waste>

---

### Question: 597

---

A new service desk is having a difficult time managing the volume of requests. Which of the following is the BEST solution for the department?

- A . Implementing a support portal
- B . Creating a ticketing system
- C . Commissioning an automated callback system
- D . Submitting tickets through email

---

**Answer: A**

---

Explanation:

A support portal is an online system that allows customers to access customer service tools, submit requests and view status updates, as well as access information such as how-to guides, FAQs, and other self-service resources. This would be the best solution for the service desk, as it would allow them to easily manage the volume of requests by allowing customers to submit their own requests and view the status of their requests. Additionally, the portal would provide customers with self-service resources that can help them resolve their own issues, reducing the amount of tickets that need to be handled by the service desk.

---

### **Question: 598**

---

A technician receives a call from a user who is on vacation. The user provides the necessary credentials and asks the technician to log in to the user's account and read a critical email that the user has been expecting. The technician refuses because this is a violation of the:

- A . acceptable use policy.
- B . regulatory compliance requirements.
- C . non-disclosure agreement
- D . incident response procedures

---

**Answer: A**

---

Explanation:

Logging into a user's account without their explicit permission is a violation of the acceptable use policy, which outlines the rules and regulations by which a user must abide while using a computer system. By logging into the user's account without their permission, the technician would be violating this policy. Additionally, this action could be seen as a breach of confidentiality, as the technician would have access to information that should remain confidential.

---

### **Question: 599**

---

A technician connects an additional monitor to a PC using a USB port. The original HDMI monitor is mounted to the left of the new monitor. When moving the mouse to the right from the original monitor to the new monitor, the mouse stops at the end of the screen on the original monitor. Which

of the following will allow the mouse to correctly move to the new monitor?

- A . Rearranging the monitor's position in display settings
- B . Swapping the cables for the monitors
- C . Using the Ctrl+Alt+> to correct the display orientation
- D . Updating the display drivers for the video card

---

**Answer: B**

---

Explanation:

The correct answer is B. Swapping the cables for the monitors. When the second monitor is connected with the HDMI port, it is necessary to swap the cables for the monitors so that the mouse can move from the original monitor to the new monitor. This is because the HDMI port is designed to only support one monitor, and the mouse will not be able to move from one to the other without the cables being swapped.

According to CompTIA A+ Core 2 documents, 'When connecting multiple displays to a system, the cables used to connect the displays must be swapped between the displays. For example, if a monitor is connected to a system using a VGA cable, the VGA cable must be moved to the next display to allow the mouse to move between the two displays.'

---

### **Question: 600**

---

An organization's Chief Financial Officer (CFO) is concerned about losing access to very sensitive, legacy unmaintained PII on a workstation if a

ransomware outbreak occurs. The CFO has a regulatory requirement to retain this data for many years. Which of the following backup methods

would BEST meet the requirements?

- A . A daily, incremental backup that is saved to the corporate file server
- B . An additional, secondary hard drive in a mirrored RAID configuration
- C . A full backup of the data that is stored off site in cold storage
- D . Weekly, differential backups that are stored in a cloud-hosting provider

---

### **Answer: C**

---

Explanation:

According to CompTIA A+ Core 2 objectives, a full backup stored off-site provides the greatest protection against data loss in the event of a ransomware attack or other data disaster. By storing the backup in a separate physical location, it is less likely to be affected by the same event that could cause data loss on the original system. Cold storage is a term used for data archiving, which typically refers to a long-term storage solution that is used for retaining data that is infrequently accessed, but still needs to be kept for regulatory or compliance reasons.

---

### **Question: 601**

---

A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

- A . Security and Maintenance
- B . Network and Sharing Center
- C . Windows Defender Firewall
- D . Internet Options

---

**Answer: D**

---

Explanation:

The best choice for accessing the necessary configuration to configure the desktop systems to use a new proxy server is the Internet Options utility. This utility can be found in the Control Panel and allows you to configure the proxy settings for your network connection. As stated in the CompTIA A+ Core 2 exam objectives, technicians should be familiar with the Internet Options utility and how to configure proxy settings.

---

**Question: 602**

---

A technician is reimaging a desktop PC. The technician connects the PC to the network and powers it on. The technician attempts to boot the computer via the NIC to image the computer, but this method does not work. Which of the following is the MOST likely reason the computer is unable to boot into the imaging system via the network?

- A . The computer's CMOS battery failed.
- B . The computer's NIC is faulty.
- C . The PXE boot option has not been enabled
- D . The Ethernet cable the technician is using to connect the desktop to the network is faulty.

---

**Answer: C**

---

Explanation:

The most likely reason the computer is unable to boot into the imaging system via the network is that the PXE boot option has not been enabled. PXE (Preboot Execution Environment) is an environment that allows computers to boot up over the network, instead of from a local disk. In order for this to work, the PXE boot option must be enabled in the computer's BIOS settings. As stated in the CompTIA A+ Core 2 exam objectives, technicians should know how to enable PXE in BIOS to enable network booting on a computer.

---

**Question: 603**

---

A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a

button labeled Accept Which of the following agreements IS MOST likely in use?

- A . DRM
- B . NDA
- C . EULA
- D . MOU

---

**Answer: C**

---

## Explanation:

The most likely agreement in use here is a EULA (End User License Agreement). This is a legally binding agreement between the user and the software developer, outlining the terms and conditions that the user must agree to in order to use the software. It is important that the user understands and agrees to the EULA before they can proceed with downloading and installing the software. As stated in the CompTIA A+ Core 2 exam objectives, users should be aware of the EULA before downloading any software.

---

### Question: 604

---

A help desk technician runs the following script: Inventory.py. The technician receives the following error message:

How do you want to Open this file?

Which of the following is the MOST likely reason this script is unable to run?

- A . Scripts are not permitted to run.
- B . The script was not built for Windows.
- C . The script requires administrator privileges,
- D . The runtime environment is not installed.

---

**Answer: D**

---

## Explanation:

The error message is indicating that the script is not associated with any program on the computer that can open and run it. This means that the script requires a runtime environment, such as Python, to be installed in order for it to execute properly. Without the appropriate runtime environment, the script will not be able to run.

---

### Question: 605

---

Which of the following file extensions are commonly used to install applications on a macOS machine? (Select THREE).

- A .mac
- B .Pkg
- C .deb
- D .dmg
- E .msi
- F .appx
- G .app
- H .apk

---

**Answer: B, D, G**

---

Explanation:

<https://support.microsoft.com/en-us/windows/common-file-name-extensions-in-windows-da4a4430-8e76-89c5-59f7-1cdbbc75cb01>

.pkg and .dmg are files used to distribute and install applications on macOS. .pkg files are installer packages that may contain multiple files and executable code, while .dmg files are disk images that can contain a single bundled application or multiple applications. .app files are typically the main executable files for macOS applications. The other options listed are file extensions for applications or installers on other platforms (such as .deb for Debian-based Linux systems, .msi for Windows, and .apk for Android). This information is covered in the Comptia A+ Core2 documents/guide under the Mac OS section.

---

### **Question: 606**

---

Which of the following data is MOST likely to be regulated?

- A . Name in a Phone book
- B . Name on a medical diagnosis
- C . Name on a job application
- D . Name on a employer's website

---

**Answer: B**

---

Explanation:

A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

---

### **Question: 607**

---

Which of the following is a consequence of end-of-life operating systems?

- A . Operating systems void the hardware warranty.
- B . Operating systems cease to function.
- C . Operating systems no longer receive updates.
- D . Operating systems are unable to migrate data to the new operating system.

---

**Answer: C**

---

Explanation:

End-of-life operating systems are those which have reached the end of their life cycle and are no longer supported by the software developer. This means that the operating system will no longer receive updates, security patches, or other new features. This can leave users vulnerable to security threats, as the system will no longer be protected against the latest threats. Additionally, this can make it difficult to migrate data to a newer operating system, as the old system is no longer supported.

---

### Question: 608

---

A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

- A . The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.
- B . The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.
- C . The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.
- D . The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

---

### Answer: D

---

Explanation:

The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS. This can be done by clicking on the Apple icon in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

---

### Question: 609

---

A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user's files?

- A . Run the virus scanner in an administrative mode.
- B . Reinstall the operating system.
- C . Reboot the system in safe mode and rescan.
- D . Manually delete the infected files.

---

### Answer: C

---

Explanation:

Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user's files.

---

### Question: 610

---

A suite of security applications was installed a few days ago on a user's home computer. The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

- A . Services in Control Panel to check for overutilization
- B . Performance Monitor to check for resource utilization
- C . System File Checker to check for modified Windows files
- D . Event Viewer to identify errors

---

**Answer: C**

---

Explanation:

[System File Checker to check for modified Windows files. System File Checker \(SFC\) is a Windows utility that can be used to scan for and restore corrupt Windows system files. SFC can be used to detect and fix any modified or corrupted system files on a computer, and thus should be checked first when a user reports that their computer has been running slowly since the installation of security applications\[1\]\[2\]. By checking SFC, any modified or corrupted system files can be identified and fixed, potentially improving the overall performance of the computer.](#)

---

### Question: 611

---

A desktop support technician is tasked with migrating several PCs from Windows 7 Pro to Windows 10 Pro. The technician must ensure files and user preferences are retained, must perform the operation locally, and should migrate one station at a time. Which of the following methods would be MOST efficient?

- A . Golden image
- B . Remote network install
- C . In-place upgrade
- D . Clean install

---

**Answer: C**

---

Explanation:

An in-place upgrade is the most efficient method for migrating from Windows 7 Pro to Windows 10 Pro, as it will retain all user files and preferences, can be done locally, and can be done one station at a time. An in-place upgrade involves installing the new version of Windows over the existing version, and can be done quickly and easily.

---

## **Question: 612**

---

A field technician applied a Group Policy setting to all the workstations in the network. This setting forced the workstations to use a specific SNTP server. Users are unable to log in now. Which of the following is the MOST likely cause of this issue?

- A . The SNTP server is offline.
- B . A user changed the time zone on a local machine.
- C . The Group Policy setting has disrupted domain authentication on the system,
- D . The workstations and the authentication server have a system clock difference.

---

**Answer: D**

---

Explanation:

The workstations and the authentication server have a system clock difference. If a Group Policy setting is applied that forces the workstations to use a specific SNTP server, but the system clock on the workstations and the authentication server are out of sync, then this can cause authentication issues and users will be unable to log in. In this case, the most likely cause of the issue is a difference in system clocks and the technician should ensure that the clocks on the workstations and the authentication server are in sync.

---

## **Question: 613**

---

A technician has been asked to set up a new wireless router with the best possible security. Which of the following should the technician implement?

- A . WPS
- B . TKIP
- C . WPA3
- D . WEP

---

**Answer: C**

---

Explanation:

WPA3 (Wi-Fi Protected Access version 3) is the latest version of Wi-Fi security and offers the highest level of protection available. It is designed to protect against brute force password attempts and protect against eavesdropping and man-in-the-middle attacks. WPA3 also supports the use of stronger encryption algorithms, such as the Advanced Encryption Standard (AES), which provides additional protection for wireless networks. WPA3 should be implemented in order to ensure the best possible security for the new wireless router.

---

## **Question: 614**

---

The findings from a security audit indicate the risk of data loss from lost or stolen laptops is high. The company wants to reduce this risk with minimal impact to users who want to use their laptops when not on the network. Which of the following would BEST reduce this risk for Windows laptop users?

- A . Requiring strong passwords
- B . Disabling cached credentials
- C . Requiring MFA to sign on
- D . Enabling BitLocker on all hard drives

---

**Answer: D**

---

Explanation:

BitLocker is a disk encryption tool that can be used to encrypt the hard drive of a Windows laptop. This will protect the data stored on the drive in the event that the laptop is lost or stolen, and will help to reduce the risk of data loss. Additionally, BitLocker can be configured to require a PIN or other authentication in order to unlock the drive, providing an additional layer of security.

---

### **Question: 615**

---

An analyst needs GUI access to server software running on a macOS server. Which of the following options provides the BEST way for the analyst to access the macOS server from the Windows workstation?

- A . RDP through RD Gateway
- B . Apple Remote Desktop
- C . SSH access with SSH keys
- D . VNC with username and password

---

**Answer: B**

---

Explanation:

Apple Remote Desktop is a remote access solution that allows a user to access and control another macOS computer from their Windows workstation. It provides a graphical user interface so that the analyst can easily access the server software running on the macOS server. Apple Remote Desktop also supports file transfers, so the analyst can easily transfer files between the two computers. Additionally, Apple Remote Desktop supports encryption, so data is secure during transmission.

---

### **Question: 616**

---

A technician is tasked with configuring a computer for a visually impaired user. Which of the following utilities should the technician use?

- A . Device Manager
- B . System

- C . Ease of Access Center
- D . Programs and Features

---

**Answer: C**

---

Explanation:

The Ease of Access Center is a built-in utility in Windows that provides tools and options for making a computer easier to use for individuals with disabilities, including the visually impaired. In the Ease of Access Center, the technician can turn on options like high contrast display, screen magnification, and screen reader software to help the user better interact with the computer.

---

### **Question: 617**

---

A user is attempting to browse the internet using Internet Explorer. When trying to load a familiar web page, the user is unexpectedly redirected to an unfamiliar website. Which of the following would MOST likely solve the issue?

- A . Updating the operating system
- B . Changing proxy settings
- C . Reinstalling the browser
- D . Enabling port forwarding

---

**Answer: C**

---

Explanation:

Reinstalling the browser would most likely solve the issue. This would remove any malicious software or add-ons that may be causing the issue and restore the browser to its default settings.

---

### **Question: 618**

---

A user received the following error upon visiting a banking website:

The security presented by website was issued a different website's address .

A technician should instruct the user to:

- A . clear the browser cache and contact the bank.
- B . close out of the site and contact the bank.
- C . continue to the site and contact the bank.
- D . update the browser and contact the bank.

---

**Answer: A**

---

### **Explanation:**

The technician should instruct the user to clear the browser cache and contact the bank (option A). This error indicates that the website the user is visiting is not the correct website and is likely due to a cached version of the website being stored in the user's browser. Clearing the browser cache should remove any stored versions of the website and allow the user to access the correct website. The user should also contact the bank to confirm that they are visiting the correct website and to report the error.

---

### **Question: 619**

---

A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

- A . The user is not connected to the VPN.
- B . The file server is offline.
- C . A low battery is preventing the connection.
- D . The log-in script failed.

---

**Answer: A**

---

---

### **Question: 620**

---

A technician is setting up a new laptop for an employee who travels. Which of the following is the BEST security practice for this scenario?

- A . PIN-based login
- B . Quarterly password changes
- C . Hard drive encryption
- D . A physical laptop lock

---

**Answer: C**

---

### **Explanation:**

Encrypting the laptop's hard drive will ensure that any sensitive data stored on the laptop is secure, even if the laptop is lost or stolen. Encryption ensures that the data cannot be accessed by anyone without the correct encryption key. This is an important security measure for any laptop used by an employee who travels, as it helps to protect the data stored on the laptop from unauthorized access.

---

### **Question: 621**

---

A technician is troubleshooting a lack of outgoing audio on a third-party Windows 10 VoIP application. The PC uses a USB microphone connected to a powered hub. The technician verifies the microphone works on the PC using Voice Recorder. Which of the following should the technician do to solve the issue?

- A . Remove the microphone from the USB hub and plug it directly into a USB port on the PC.
- B . Enable the microphone under Windows Privacy settings to allow desktop applications to access it.
- C . Delete the microphone from Device Manager and scan for new hardware,
- D . Replace the USB microphone with one that uses a traditional 3.5mm plug.

---

**Answer: B**

---

Explanation:

In Windows 10, there are privacy settings that control access to certain devices, such as microphones, cameras, and other input devices. If the microphone is not enabled under these privacy settings, the VoIP application may not have access to it, causing a lack of outgoing audio.

The technician can go to the Windows 10 Settings menu, select the Privacy submenu, and under App permissions, select Microphone. The technician should then turn on the toggle switch for the VoIP application to allow it to access the microphone.

Removing the microphone from the USB hub and plugging it directly into a USB port on the PC may or may not solve the issue, as the issue could be related to the privacy settings. Deleting the microphone from Device Manager and scanning for new hardware may also not solve the issue, as the issue could be related to the privacy settings. Replacing the USB microphone with one that uses a traditional 3.5mm plug is not recommended, as it would require purchasing a new microphone and may not solve the issue.

---

### **Question: 622**

---

A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

- A . Differential backup
- B . Off-site backup
- C . Incremental backup
- D . Full backup

---

**Answer: D**

---

Explanation:

A full backup involves creating a copy of all data on the workstation, including system files and user-created data, and storing it on a set of tapes. This ensures that all data is backed up, and ensures that the data can be restored in the event of a system failure or data loss.

---

### **Question: 623**

---

A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application

was installed on the phone. Which of the following is the MOST likely cause?

- A . The GPS application is installing software updates.
- B . The GPS application contains malware.
- C . The GPS application is updating its geospatial map data.
- D . The GPS application is conflicting with the built-in GPS.

---

**Answer: B**

---

Explanation:

The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phone1

---

### **Question: 624**

---

Which of the following is the MOST basic version of Windows that includes BitLocker?

- A . Home
- B . pro
- C . Enterprise
- D . Pro for Workstations

---

**Answer: D**

---

Explanation:

The most basic version of Windows that includes BitLocker is Windows Pro. BitLocker is a feature of Windows Pro that provides full disk encryption for all data on a storage drive[1]. It helps protect data from unauthorized access or theft and can help secure data from malicious attacks. Pro for Workstations includes this feature, as well as other features such as support for up to 6 TB of RAM and ReFS.

---

### **Question: 625**

---

Security software was accidentally uninstalled from all servers in the environment. After requesting the same version of the software be reinstalled, the security analyst learns that a change request will need to be filled out. Which of the following is the BEST reason to follow the change management process in this scenario?

- A . Owners can be notified a change is being made and can monitor it for performance impact. Most Voted
- B . A risk assessment can be performed to determine if the software is needed.
- C . End users can be aware of the scope of the change.
- D . A rollback plan can be implemented in case the software breaks an application.

---

**Answer: A**

---

Explanation:

change management process can help ensure that owners are notified of changes being made and can monitor them for performance impact (A). This can help prevent unexpected issues from arising.

---

### **Question: 626**

---

While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?

- A . A bad antivirus signature update was installed.
- B . A router was misconfigured and was blocking traffic.
- C . An upstream internet service provider was flapping.
- D . The time or date was not in sync with the website.

---

**Answer: B**

---

Explanation:

The most likely cause of this issue is that a router was misconfigured and was blocking traffic. This would explain why remote users who were not connected to corporate resources did not have any issues.

---

### **Question: 627**

---

A company discovered that numerous computers from multiple geographic locations are sending a very high number of connection requests which is causing the company's web server to become unavailable to the general public. Which of the following attacks is occurring?

- A . Zero day
- B . SQL injection
- C . Cross-site scripting
- D . Distributed denial of service

---

**Answer: D**

---

Explanation:

The company is experiencing a distributed denial of service (DDoS) attack. A DDoS attack is a type of cyber attack in which multiple compromised systems are used to target a single system, causing a denial of service for users of the

targeted system.

---

### Question: 628

---

While assisting a customer with an issue, a support representative realizes the appointment is taking longer than expected and will cause the next customer meeting to be delayed by five minutes. Which of the following should the support representative do NEXT?

- A . Send a quick message regarding the delay to the next customer.
- B . Cut the current customer's lime short and rush to the next customer.
- C . Apologize to the next customer when arriving late.
- D . Arrive late to the next meeting without acknowledging the lime.

---

**Answer: A**

---

Explanation:

The support representative should send a quick message regarding the delay to the next customer. This will help the next customer understand the situation and adjust their schedule accordingly.

---

### Question: 629

---

A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore times but asks the technician to retain more versions when possible. Which of the following backup methods should the technician MOST likely implement?

- A . Full
- B . Mirror
- C . Incremental
- D . Differential

---

**Answer: C**

---

Explanation:

The law firm wants to retain more versions of the backups when possible, so the best backup method for the technician to implement in this scenario would be Incremental backup. Incremental backups only save the changes made since the last backup, which allows for more frequent backups and minimizes the amount of storage required. This would allow the law firm to retain more than three versions of backups without risking backup failure.

To retain more versions of backups, the technician should implement an Incremental backup method12

An incremental backup method only backs up the data that has changed since the last backup, so it requires less storage space than a full backup12

---

### **Question: 630**

---

A technician has just used an anti-malware removal tool to resolve a user's malware issue on a corporate laptop. Which of the following BEST describes what the technician should do before returning the laptop to the user?

- A . Educate the user on malware removal.
- B . Educate the user on how to reinstall the laptop OS.
- C . Educate the user on how to access recovery mode.
- D . Educate the user on common threats and how to avoid them.

---

**Answer: D**

---

Explanation:

educating the user on common threats and how to avoid them (D) would be a good step before returning the laptop to the user. This can help prevent similar issues from happening again.

---

### **Question: 631**

---

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

- A . File Explorer
- B . User Account Control
- C . Windows Backup and Restore
- D . Windows Firewall
- E . Windows Defender
- F . Network Packet Analyzer

---

**Answer: A, E**

---

Explanation:

[The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software1](#)

---

### **Question: 632**

---

Which of the following should be done NEXT?

- A . Send an email to Telecom to inform them of the issue and prevent reoccurrence.

- B . Close the ticket out.
- C . Tell the user to take time to fix it themselves next time.
- D . Educate the user on the solution that was performed.

---

**Answer: D**

---

Explanation:

educating the user on the solution that was performed is a good next step after resolving an issue. This can help prevent similar issues from happening again and empower users to solve problems on their own.

---

### **Question: 633**

---

A user turns on a new laptop and attempts to log in to specialized software, but receives a message stating that the address is already in use. The user logs on to the old desktop and receives the same message. A technician checks the account and sees a comment that the user requires a specifically allocated address before connecting to the software. Which of the following should the technician do to MOST likely resolve the issue?

- A . Bridge the LAN connection between the laptop and the desktop.
- B . Set the laptop configuration to DHCP to prevent conflicts.
- C . Remove the static IP configuration from the desktop.
- D . Replace the network card in the laptop, as it may be defective.

---

**Answer: C**

---

Explanation:

The new laptop was set up with the static IP it needs to connect to the software. The old desktop is still configured with that IP, hence the conflict.

---

### **Question: 634**

---

A help desk team lead contacts a systems administrator because the technicians are unable to log in to a Linux server that is used to access tools. When the administrator tries to use remote desktop to log in to the server, the administrator sees the GUI is crashing. Which of the following methods can the administrator use to troubleshoot the server effectively?

- A . SFTP
- B . SSH
- C . VNC
- D . MSRA

---

**Answer: C**

---

Explanation:

The administrator can use Virtual Network Computing (VNC) to troubleshoot the server effectively. VNC is a graphical desktop sharing system that allows the administrator to remotely control the desktop of a Linux server.

---

### Question: 635

---

A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

- A . Differential backup
- B . Off-site backup
- C . Incremental backup
- D . Full backup

---

**Answer: D**

---

Explanation:

[To accomplish this task, the technician should use aFull backupmethod1](#)

[A full backup only requires two sets of tapes to restore because it backs up all the data from the workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data1](#)

---

### Question: 636

---

A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

- A . Encrypt the workstation hard drives.
- B . Lock the workstations after five minutes of inactivity.
- C . Install privacy screens.
- D . Log off the users when their workstations are not in use.

---

**Answer: B**

---

Explanation:

The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from accessing patient data if call center agents were to step away from their workstations without logging out.

---

### **Question: 637**

---

A police officer often leaves a workstation for several minutes at a time. Which of the following is the BEST way the officer can secure the workstation quickly when walking away?

- A . Use a key combination to lock the computer when leaving.
- B . Ensure no unauthorized personnel are in the area.
- C . Configure a screensaver to lock the computer automatically after approximately 30 minutes of inactivity.
- D . Turn off the monitor to prevent unauthorized visibility of information.

---

**Answer: A**

---

Explanation:

[The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving1](#)

---

### **Question: 638**

---

Which of the following command-line tools will delete a directory?

- A . md
- B . del
- C . dir
- D . rd
- E . cd

---

**Answer: D**

---

Explanation:

To delete an empty directory, enter rd Directory or rmdir Directory . If the directory is not empty, you can remove files and subdirectories from it using the /s switch. You can also use the /q switch to suppress confirmation messages (quiet mode).

---

### **Question: 639**

---

Which of the following is an example of MFA?

- A . Fingerprint scan and retina scan
- B . Password and PIN
- C . Username and password
- D . Smart card and password

---

**Answer: D**

---

Explanation:

Smart card and password is an example of two-factor authentication (2FA), not multi-factor authentication (MFA). MFA requires two or more authentication factors.Smart card and password is an example of two-factor authentication (2FA)2

---

### **Question: 640**

---

A user is having issues with document-processing software on a Windows workstation. Other users that log in to the same device do not have the same issue.

Which of the following should a technician do to remediate the issue?

- A . Roll back the updates.
- B . Increase the page file.
- C . Update the drivers.
- D . Rebuild the profile.

---

**Answer: D**

---

Explanation:

The issue is specific to the user's profile, so the technician should rebuild the profile.Rebuilding the profile will create a new profile and transfer the user's data to the new profile1

---

### **Question: 641**

---

A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which of the following files should the technician execute in order to complete the installation?

- A . Installer\_x64.exe
- B . Installer\_Files.zip
- C . Installer\_32.msi
- D . Installer\_x86.exe
- E . Installer\_Win10Enterprise.dmg

---

**Answer: D**

---

Explanation:

The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The "x86" in the file name refers to the 32-bit architecture.

<https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating-systems/>

---

### Question: 642

---

Before leaving work, a user wants to see the traffic conditions for the commute home. Which of the following tools can the user employ to schedule the browser to automatically launch a traffic website at 4:45 p.m.?

- A . taskschd.msc
- B . perfmon.msc
- C . lusrmgr.msc
- D . Eventvwr.msc

---

**Answer: A**

---

Explanation:

The user can use the Task Scheduler (taskschd.msc) to schedule the browser to automatically launch a traffic website at 4:45 p.m. The Task Scheduler is a tool in Windows that allows users to schedule tasks to run automatically at specified times or in response to certain events.

---

### Question: 643

---

A developer is creating a shell script to automate basic tasks in Linux. Which of the following file types are supported by default?

- A .py
- B .js
- C .vbs
- D .sh

---

**Answer: D**

---

Explanation:

<https://www.educba.com/shell-scripting-in-linux/>

---

### Question: 644

---

A user created a file on a shared drive and wants to prevent its data from being accidentally deleted by others. Which of the following applications should the technician use to assist the user with hiding the file?

- A . Device Manager
- B . Indexing Options
- C . File Explorer
- D . Administrative Tools

---

**Answer: C**

---

Explanation:

The technician should use the File Explorer application to assist the user with hiding the file1. The user can right-click the file and select Properties.In the Properties dialog box, select the Hidden check box, and then click OK1.

---

### **Question: 645**

---

A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

- A . ipconfig /all
- B . hostname
- C . netstat /?
- D . nslookup localhost
- E . arp ---a
- F . ping :: 1

---

**Answer: A, B**

---

Explanation:

The user can use the following commands to give the technician the correct information:ipconfig /all and hostname1.The ipconfig /all command displays the IP address, subnet mask, and default gateway for all adapters on the computer1.The hostname command displays the name of the computer1.

---

### **Question: 646**

---

Which of the following should be used to control security settings on an Android phone in a domain environment?

- A . MDM
- B . MFA
- C . ACL
- D . SMS

---

**Answer: A**

---

Explanation:

The best answer to control security settings on an Android phone in a domain environment is to use "Mobile Device Management (MDM)". MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can be used to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities<sup>12</sup>

---

### **Question: 647**

---

Which of the following is a data security standard for protecting credit cards?

- A . PHI
- B . NIST
- C . PCI
- D . GDPR

---

**Answer: C**

---

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

---

### **Question: 648**

---

A technician just completed a Windows 10 installation on a PC that has a total of 16GB of RAM. The technician notices the Windows OS has only 4GB of RAM available for use. Which of the following explains why the OS can only access 4GB of RAM?

- A . The UEFI settings need to be changed.
- B . The RAM has compatibility issues with Windows 10.
- C . Some of the RAM is defective.
- D . The newly installed OS is x86.

---

**Answer: D**

---

Explanation:

The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. The x64 version of Windows 10 can use up to 2TB of RAM<sup>13</sup>.

---

### **Question: 649**

---

A technician is working to resolve a Wi-Fi network issue at a doctor's office that is located next to an apartment complex. The technician discovers that employees and patients are not the only people on the network. Which of the following should the technician do to BEST minimize this issue?

- A . Disable unused ports.
- B . Remove the guest network
- C . Add a password to the guest network
- D . Change the network channel.

---

**Answer: D**

---

Explanation:

[Changing the network channel is the best solution to minimize the issue of employees and patients not being the only people on the Wi-Fi network5](#)

---

### **Question: 650**

---

A bank would like to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. Which of the following BEST addresses this need?

- A . Guards
- B . Bollards
- C . Motion sensors
- D . Access control vestibule

---

**Answer: B**

---

Explanation:

[Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers4](#)

---

### **Question: 651**

---

A network administrator is deploying a client certificate to be used for Wi-Fi access for all devices in an organization. The certificate will be used in conjunction with the user's existing username and password. Which of the following BEST describes the security benefits realized after this deployment?

- A . Multifactor authentication will be forced for Wi-Fi
- B . All Wi-Fi traffic will be encrypted in transit
- C . Eavesdropping attempts will be prevented
- D . Rogue access points will not connect

---

**Answer: A**

---

Explanation:

[Multifactor authentication will be forced for Wi-Fi after deploying a client certificate to be used for Wi-Fi access for all devices in an organization3](#)

CompTIA Security+ (Plus) Practice Test Questions | CompTIA. Retrieved from  
<https://www.comptia.org/training/resources/comptia-security-practice-tests>

Topic 2, Exam Pool B

---

### **Question: 652**

---

A company needs to securely dispose of data stored on optical discs. Which of the following is the MOST effective method to accomplish this task?

- A . Degaussing
- B . Low-level formatting
- C . Recycling
- D . Shredding

---

**Answer: D**

---

Explanation:

[Shredding is the most effective method to securely dispose of data stored on optical discs12](#)

---

### **Question: 653**

---

A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email. The technician asks the user to describe any unusual activity, such as slow performance, excessive pop-ups, and browser redirections. Which of the following should the technician do NEXT?

- A . Advise the user to run a complete system scan using the OS anti-malware application
- B . Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still present
- C . Have the user check for recently installed applications and outline those installed since the link in the email was clicked
- D . Instruct the user to disconnect the Ethernet connection to the corporate network.

---

**Answer: D**

---

Explanation:

First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn't spread.

---

### Question: 654

---

A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?

- A . Rights management
- B . Audit trail
- C . Chain of custody
- D . Data integrity

---

**Answer: C**

---

Explanation:

[The process of documenting who had possession of evidence at every step of the process is called chain of custody.](#)

---

### Question: 655

---

An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

- A . Uninstall and reinstall the application
- B . Reset the phone to factory settings
- C . Install an alternative application with similar functionality
- D . Clear the application cache.

---

**Answer: D**

---

Explanation:

[The systems administrator should clear the application cache12](#)

[If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application12](#)

[Resetting the phone to factory settings is not necessary at this point12](#)

[Installing an alternative application with similar functionality is not necessary at this point12](#)

---

## **Question: 656**

---

A user purchased a netbook that has a web-based, proprietary operating system. Which of the following operating systems is MOST likely installed on the netbook?

- A . macOS
- B . Linux
- C . Chrome OS
- D . Windows

---

**Answer: C**

---

Explanation:

[4. Chrome OS.](https://en.wikipedia.org/wiki/Chrome_OS) Retrieved from [https://en.wikipedia.org/wiki/Chrome\\_OS](https://en.wikipedia.org/wiki/Chrome_OS) 5. What is Chrome OS? Retrieved from <https://www.google.com/chromebook/chrome-os/>

A netbook with a web-based, proprietary operating system is most likely running Chrome OS. Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low-power devices and is designed to be fast, secure, and easy to use.

---

## **Question: 657**

---

A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

- A . FAT32
- B . ext4
- C . NTFS
- D . exFAT

---

**Answer: D**

---

Explanation:

[exFAT is a file system that is supported by both Linux and Windows and can handle large files1.](#)

---

## **Question: 658**

---

A Chief Executive Officer has learned that an exploit has been identified on the web server software, and a patch is not available yet. Which of the following attacks MOST likely occurred?

- A . Brute force
- B . Zero day
- C . Denial of service

D . On-path

---

**Answer: B**

---

Explanation:

A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability.

Configuring AAA Services. Retrieved from [https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs\\_r4-0/security/configuration/guide/sc40crsbook\\_chapter1.html](https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsbook_chapter1.html)

---

### **Question: 659**

---

A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. Which of the following should the technician implement?

- A . MSRA
- B . VNC
- C . VPN
- D . SSH

---

**Answer: C**

---

Explanation:

A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. The technician should implement VPN

---

### **Question: 660**

---

Which of the following is a proprietary Cisco AAA protocol?

- A . TKIP
- B . AES
- C . RADIUS
- D . TACACS+

---

**Answer: D**

---

Explanation:

TACACS+ is a proprietary Cisco AAA protocol

---

### **Question: 661**

---

A user receives a notification indicating the antivirus protection on a company laptop is out of date. A technician is able to ping the user's laptop. The technician checks the antivirus parent servers and sees the latest signatures have been installed. The technician then checks the user's laptop and finds the antivirus engine and definitions are current. Which of the following has MOST likely occurred?

- A . Ransomware
- B . Failed OS updates
- C . Adware
- D . Missing system files

---

**Answer: B**

---

Explanation:

The most likely reason for the antivirus protection on a company laptop being out of date is failed OS updates1.  
Antivirus software relies on the operating system to function properly.If the operating system is not up-to-date, the  
antivirus software may not function properly and may not be able to receive the latest virus definitions and  
updates2.Therefore, it is important to keep the operating system up-to-date to ensure the antivirus software is  
functioning properly2.

---

### **Question: 662**

---

A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

- A . The hardware does not meet BitLocker's minimum system requirements.
- B . BitLocker was renamed for Windows 10.
- C . BitLocker is not included on Windows 10 Home.
- D . BitLocker was disabled in the registry of the laptop

---

**Answer: C**

---

Explanation:

BitLocker is only available on Windows 10 Pro, Enterprise, and Education editions1.  
Therefore, the technician is unable to find the BitLocker Drive Encryption menu item in Control Panel because it is not included in the Windows 10 Home edition1.

---

### **Question: 663**

---

A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?

- A . Open Settings, select Accounts, select, Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper
- B . Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper
- C . Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper
- D . Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.

---

**Answer: B**

---

Explanation:

[To change the desktop wallpaper on a Windows 10 computer using a Windows 10 Settings tool, the user should openSettings, selectPersonalization, clickBrowse, and then locate and open the image the user wants to use as the wallpaper1](#)

<https://www.lifewire.com/change-desktop-background-windows-11-5190733>

---

### **Question: 664**

---

A technician suspects the boot disk of a user's computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?

- A . Run sfc / scannow on the drive as the administrator.
- B . Run clearnmgr on the drive as the administrator
- C . Run chkdsk on the drive as the administrator.
- D . Run dfrgui on the drive as the administrator.

---

**Answer: C**

---

Explanation:

The technician should verify bad sectors on the user's computer by running chkdsk on the drive as the administrator. Chkdsk (check disk) is a command-line utility that detects and repairs disk errors, including bad sectors. It runs a scan of the disk and displays any errors that are found

---

### **Question: 665**

---

Which of the following Linux commands would be used to install an application?

- A . yum

- B . grep
- C . ls
- D . sudo

---

**Answer: D**

---

Explanation:

The Linux command used to install an application is sudo. The sudo command allows users to run programs with the security privileges of another user, such as the root user. This is necessary to install applications because it requires administrative privileges1

---

### **Question: 666**

---

A technician is installing new network equipment in a SOHO and wants to ensure the equipment is secured against external threats on the Internet. Which of the following actions should the technician do FIRST?

- A . Lock all devices in a closet.
- B . Ensure all devices are from the same manufacturer.
- C . Change the default administrative password.
- D . Install the latest operating system and patches

---

**Answer: C**

---

Explanation:

The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet. Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patches is important for maintaining the security of the network equipment, but it is not the first action the technician should take1

---

### **Question: 667**

---

A user reports that text on the screen is too small. The user would like to make the text larger and easier to see. Which of the following is the BEST way for the user to increase the size of text, applications, and other items using the Windows 10 Settings tool?

- A . Open Settings select Devices, select Display, and change the display resolution to a lower resolution option
- B . Open Settings, select System, select Display, and change the display resolution to a lower resolution option.
- C . Open Settings Select System, select Display, and change the Scale and layout setting to a higher percentage.
- D . Open Settings select Personalization, select Display and change the Scale and layout setting to a higher percentage

---

**Answer: C**

---

Explanation:

[Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage123](#)

---

### **Question: 668**

---

An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update. A technician determines there are no error messages on the device. Which of the following should the technician do NEXT?

- A . Verify all third-party applications are disabled
- B . Determine if the device has adequate storage available.
- C . Check if the battery is sufficiently charged
- D . Confirm a strong internet connection is available using Wi-Fi or cellular data

---

**Answer: C**

---

Explanation:

[Since there are no error messages on the device, the technician should check if the battery is sufficiently charged1](#)

[If the battery is low, the device may not have enough power to complete the update2](#)

In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process.

Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices. However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

---

### **Question: 669**

---

A user reports a computer is running slow. Which of the following tools will help a technician identify the issued

- A . Disk Cleanup
- B . Group Policy Editor
- C . Disk Management
- D . Resource Monitor

Explanation:

[Resource Monitor will help a technician identify the issue when a user reports a computer is running slow1](#)

---

## Question: 670

---

Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Click on individual tickers to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify/Resolve drop-down menu.

Details

#8675310	Open
Priority	Low
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022

Subject: Unable to access Z: on my computer, but I can manually enter the location in the window.

Attachments: [File Explorer.jpg](#)

Issue:

Resolution:

Verify/Resolve:

**Close Ticket**

**TEST QUESTION**

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Show Question

Reset All Answers

	Date	Priority
lking to boot. Screen i... 9	7/13/2022	High
o access Z: on my co... 0	7/13/2022	Low

Issue: Corrupt OS  
Resolution: Reinstall Operating System  
Verify/Resolve: chkdsk

Issue: Recent Windows Updates  
Resolution: Rollback Updates  
Verify/Resolve: dism

Issue: Graphics Drive Updates  
Resolution: Rollback Drivers  
Verify/Resolve: diskpart

Issue: BSOD  
Resolution: Repair Application  
Verify/Resolve: sfc

Issue: Printing Issues  
Resolution: Restart Print Spooler  
Verify/Resolve: dd

Issue: Limited Network Connectivity  
Resolution: Disable Network Adapter  
Verify/Resolve: ctrl + alt + del

Issue: Services Failed to Start  
Resolution: Update Network Drivers  
Verify/Resolve: net use

Issue: User Profile is Corrupted  
Resolution: Refresh DHCP  
Verify/Resolve: net user

Issue: Application Crash  
Resolution: Rebuild Windows Profile  
Verify/Resolve: netstat

Issue: User cannot access shared resource  
Resolution: Repair Installation  
Verify/Resolve: netsh

Issue: URL contains typo  
Resolution: Restore from Recovery Partition  
Verify/Resolve: bootrec

### INSTRUCTIONS

Click on individual tickets to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

Resolution: Reinstall Operating System  
Verify/Resolve: chkdsk

Resolution: Rollback Updates  
Verify/Resolve: dism

Resolution: Rollback Drivers  
Verify/Resolve: diskpart

Resolution: Repair Application  
Verify/Resolve: sfc

Resolution: Restart Print Spooler  
Verify/Resolve: dd

Resolution: Disable Network Adapter  
Verify/Resolve: ctrl + alt + del

Resolution: Update Network Drivers  
Verify/Resolve: net use

Resolution: Refresh DHCP  
Verify/Resolve: net user

Resolution: Rebuild Windows Profile  
Verify/Resolve: netstat

Resolution: Repair Installation  
Verify/Resolve: netsh

Resolution: Restore from Recovery Partition  
Verify/Resolve: bootrec

Resolution: Remap network drive  
Verify/Resolve:

Resolution: Verify integrity of disk drive  
Verify/Resolve:

Resolution: Initiate screen share session with user  
Verify/Resolve:

Resolution: Windows recovery environment  
Verify/Resolve:

Resolution: Inform user of AUP violation  
Verify/Resolve:

Verify/Resolve: chkdsk  
Verify/Resolve: dism  
Verify/Resolve: diskpart  
Verify/Resolve: sfc  
Verify/Resolve: dd  
Verify/Resolve: ctrl + alt + del  
Verify/Resolve: net use  
Verify/Resolve: net user  
Verify/Resolve: netstat  
Verify/Resolve: netsh  
Verify/Resolve: bootrec

**Answer:**

**TEST QUESTION**

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

	Date	Priority
lking to boot. Screen i... 9	7/13/2022	High
o access Z: on my co... 0	7/13/2022	Low

**INSTRUCTIONS**  
Click on individual tickets to see the ticket details. View attachments to determine the problem.  
  
Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.

If at any time you would like to bring back the Initial state of the simulation, please click the Reset All button.

**Issue**

- Corrupt OS
- Recent Windows Updates
- Graphics Drive Updates
- BSOD
- Printing Issues
- Limited Network Connectivity
- Services Failed to Start
- User Profile is Corrupted
- Application Crash
- User cannot access shared resource
- URL contains typo

**Resolution**

- Reinstall Operating System
- Rollback Updates
- Rollback Drivers
- Repair Application
- Restart Print Spooler
- Disable Network Adapter
- Update Network Drivers
- Refresh DHCP
- Rebuild Windows Profile
- Apply Updates
- Repair Installation
- Restore from Recovery Partition
- Remap network drive
- Verify integrity of disk drive
- Initiate screen share session with user
- Windows recovery environment
- Inform user of AUP violation

**Verify/Resolve**

- chkdsk
- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user
- netstat
- netsh
- bootrec

## Question: 671

Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Click on individual tickets to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify/Resolve drop-down menu.

**TEST QUESTION**

Show Question Reset All Answers

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

**Details**

Date	Priority
PC is failing to boot. Screen i... 7/13/2022	High
o access Z: on my co... 7/13/2022	Low

No Ticket Selected  
Please select a ticket from the list

**INSTRUCTIONS**

Click on individual tickets to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

**Details**

Date	Priority
PC is failing to boot. Screen i... 7/13/2022	High
o access Z: on my co... 7/13/2022	Low

#8675309      Open  
Priority      High  
Category      Technical / Bug Reports  
Assigned To      helpdesk@fictional.com  
Assigned Date      7/13/2022

Subject      PC is failing to boot. Screen is displaying error message, see attachment.  
Attachments      bootmgr\_not\_found.png

Issue

Resolution

Verify/Resolve

**Details**

Date	Priority
ing to boot. Screen i... 9	7/13/2022 <b>High</b>
o access Z: on my co... 0	7/13/2022 Low

**Subject** PC is failing to boot. Screen is displaying error message, see attachment

**Attachments** [bootmgr not found.png](#)

**Issue**

- Comupt OS
- Recent Windows Updates
- Graphics Drive Updates
- BSOD
- Printing Issues
- Limited Network Connectivity
- Services Failed to Start
- User Profile is Corrupted
- Application Crash
- User cannot access shared resource
- URL contains typo

**Resolution**

- Reinstall Operating System
- Rollback Updates
- Rollback Drivers
- Repair Application
- Restart Print Spooler
- Disable Network Adapter
- Update Network Drivers
- Refresh DHCP
- Rebuild Windows Profile
- Apply Updates
- Repair Installation
- Restore from Recovery Partition
- Remap network drive
- Verify integrity of disk drive
- Initiate screen share session with user
- Windows recovery environment
- Inform user of AUP violation

**Verify/Resolve**

- chkdsk
- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user
- netstat
- netsh
- bootrec

---

**Answer:**

---

**Details**

Date	Priority
ing to boot. Screen i... 9	7/13/2022 <b>High</b>
o access Z: on my co... 0	7/13/2022 Low

**Subject** PC is failing to boot. Screen is displaying error message, see attachment  
**Attachments** bootmgr not found.png  
**Issue**

- Corrupt OS
- Recent Windows Updates
- Graphics Drive Updates
- BSOD
- Printing Issues
- Limited Network Connectivity
- Services Failed to Start
- User Profile is Corrupted
- Application Crash
- User cannot access shared resource
- URL contains typo

**Resolution**

- Reinstall Operating System**
- Rollback Updates
- Rollback Drivers
- Repair Application
- Restart Print Spooler
- Disable Network Adapter
- Update Network Drivers
- Refresh DHCP
- Rebuild Windows Profile
- Apply Updates
- Repair Installation
- Restore from Recovery Partition
- Remap network drive
- Verify integrity of disk drive
- Initiate screen share session with user
- Windows recovery environment
- Inform user of AUP violation

**Verify/Resolve**

- chkdsk**
- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user
- netstat
- netsh
- bootrec

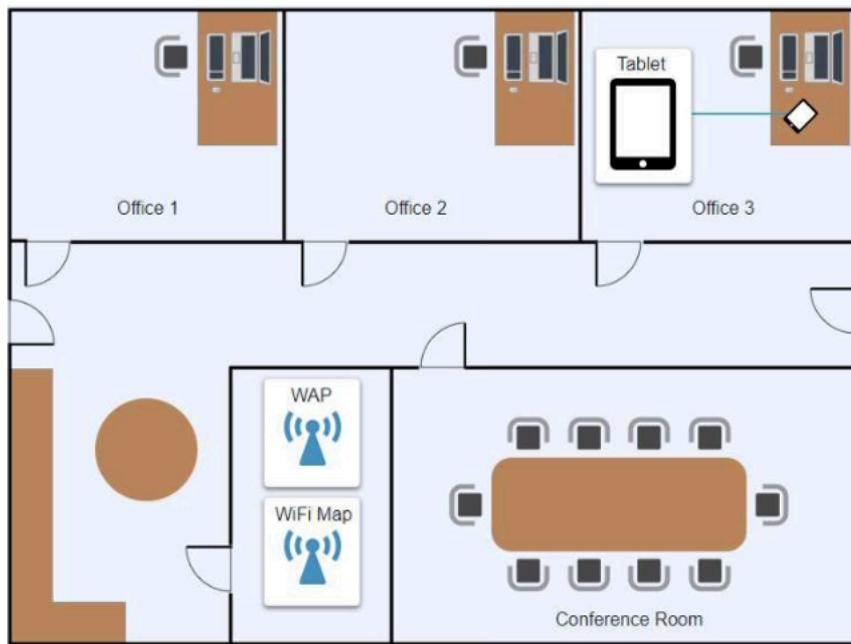
## SIMULATION

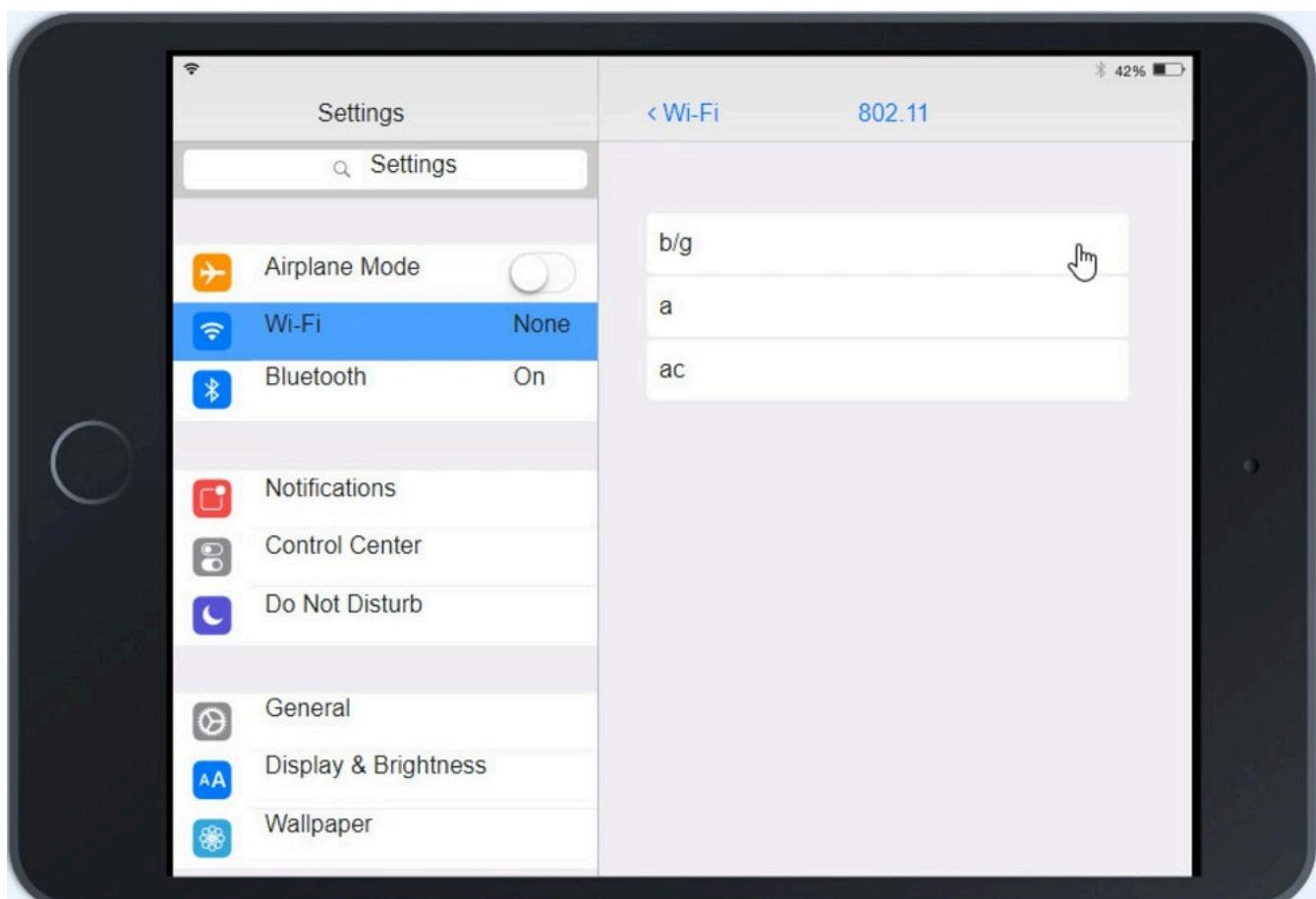
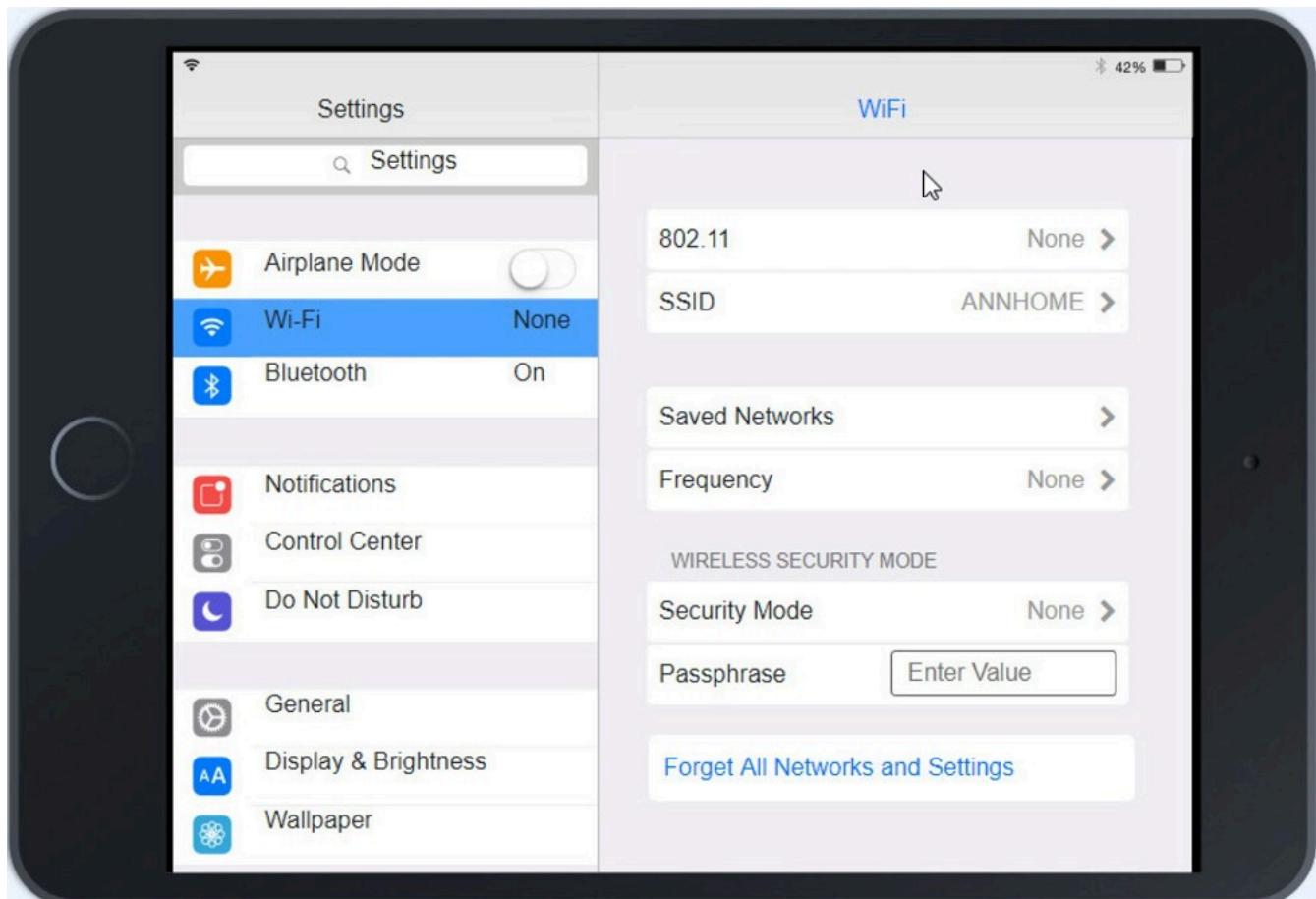
Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the company's wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.

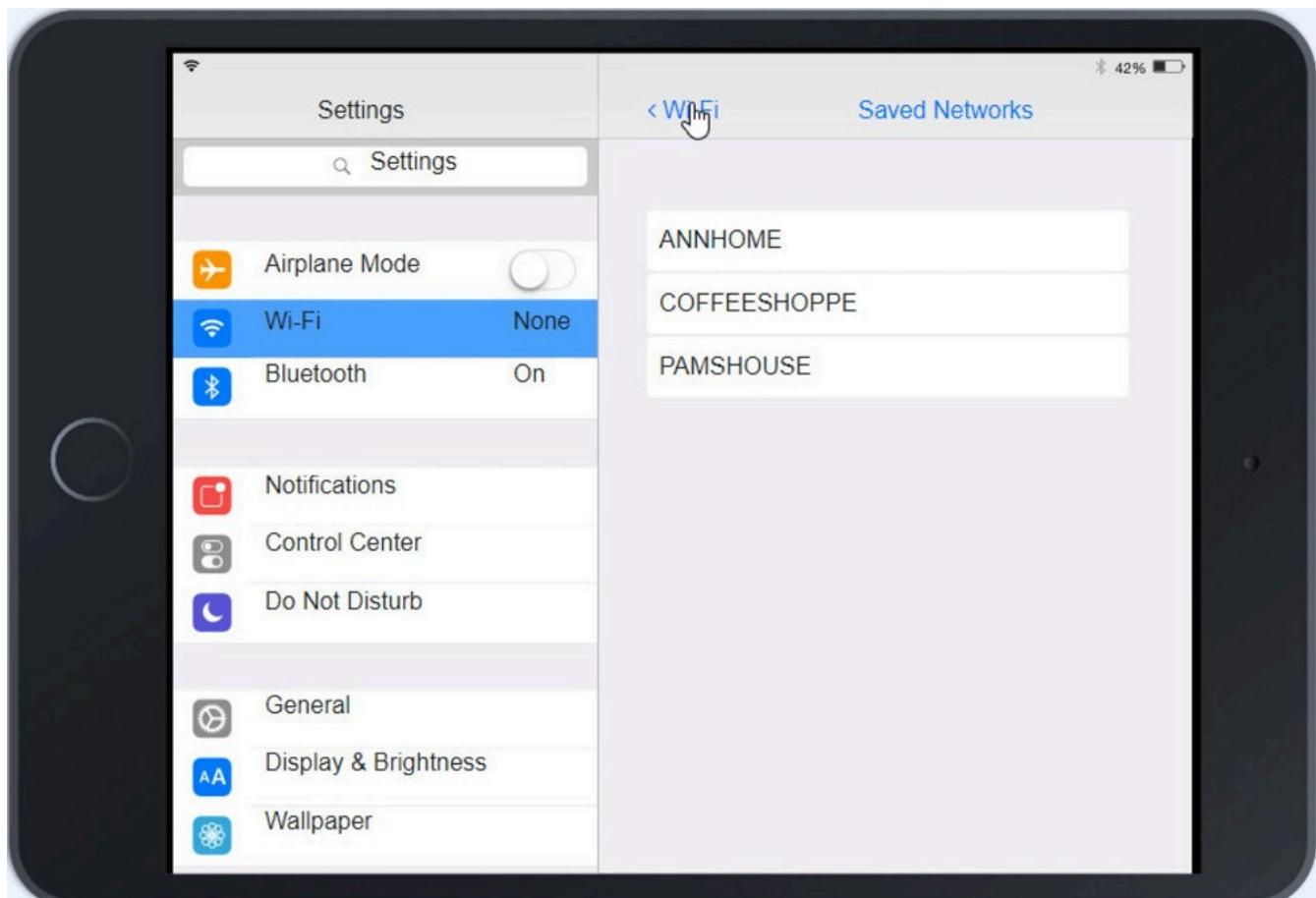
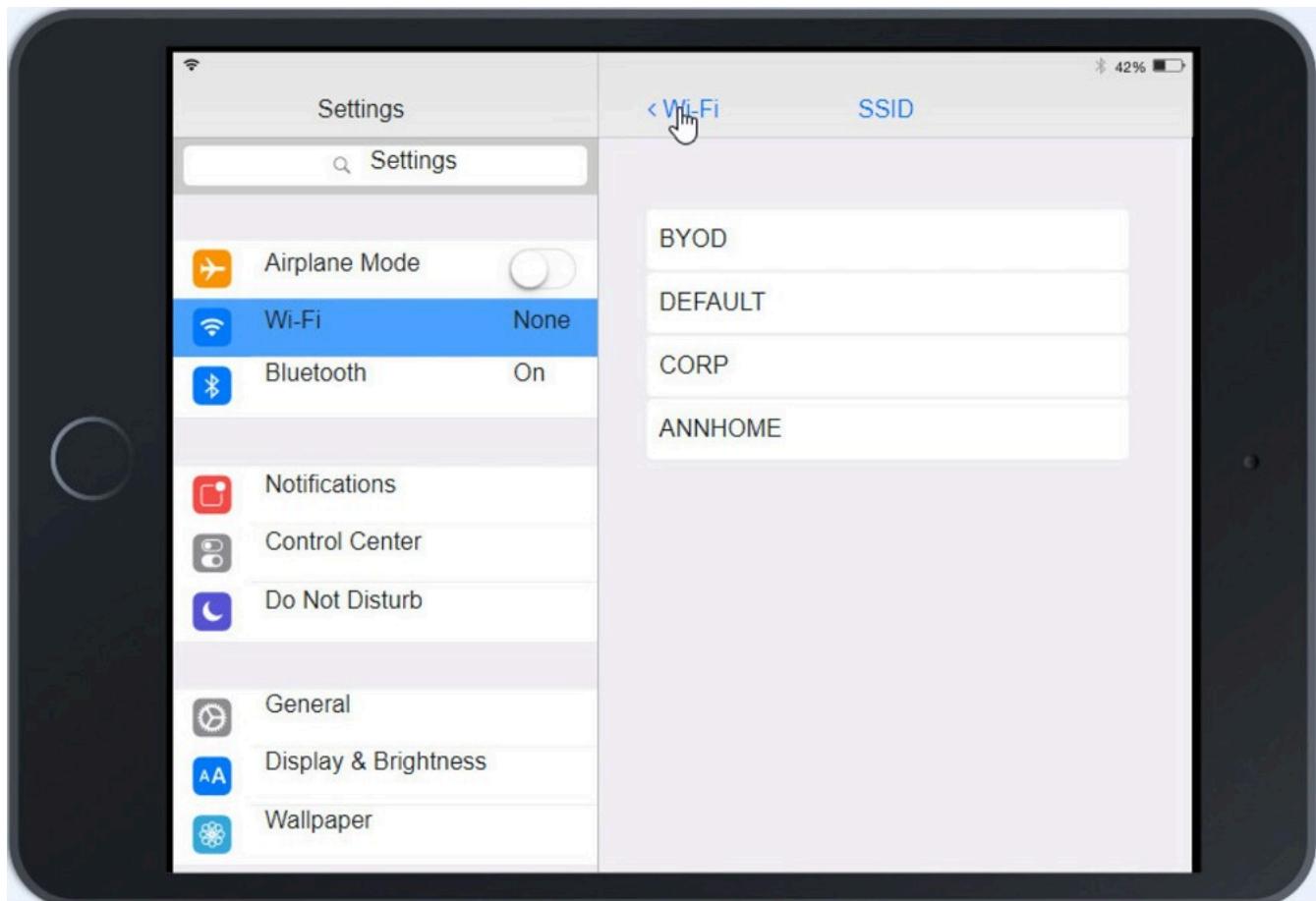
## INSTRUCTIONS

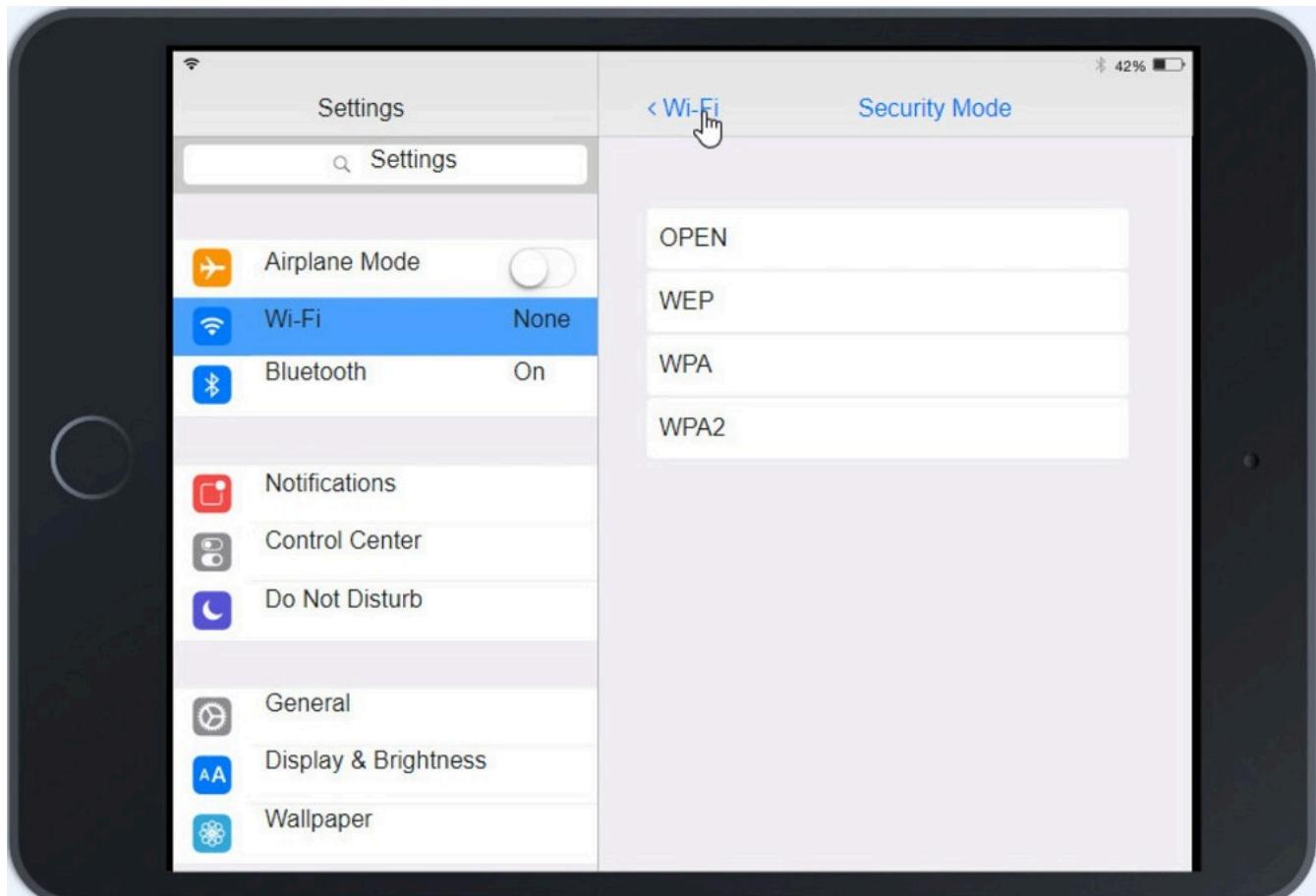
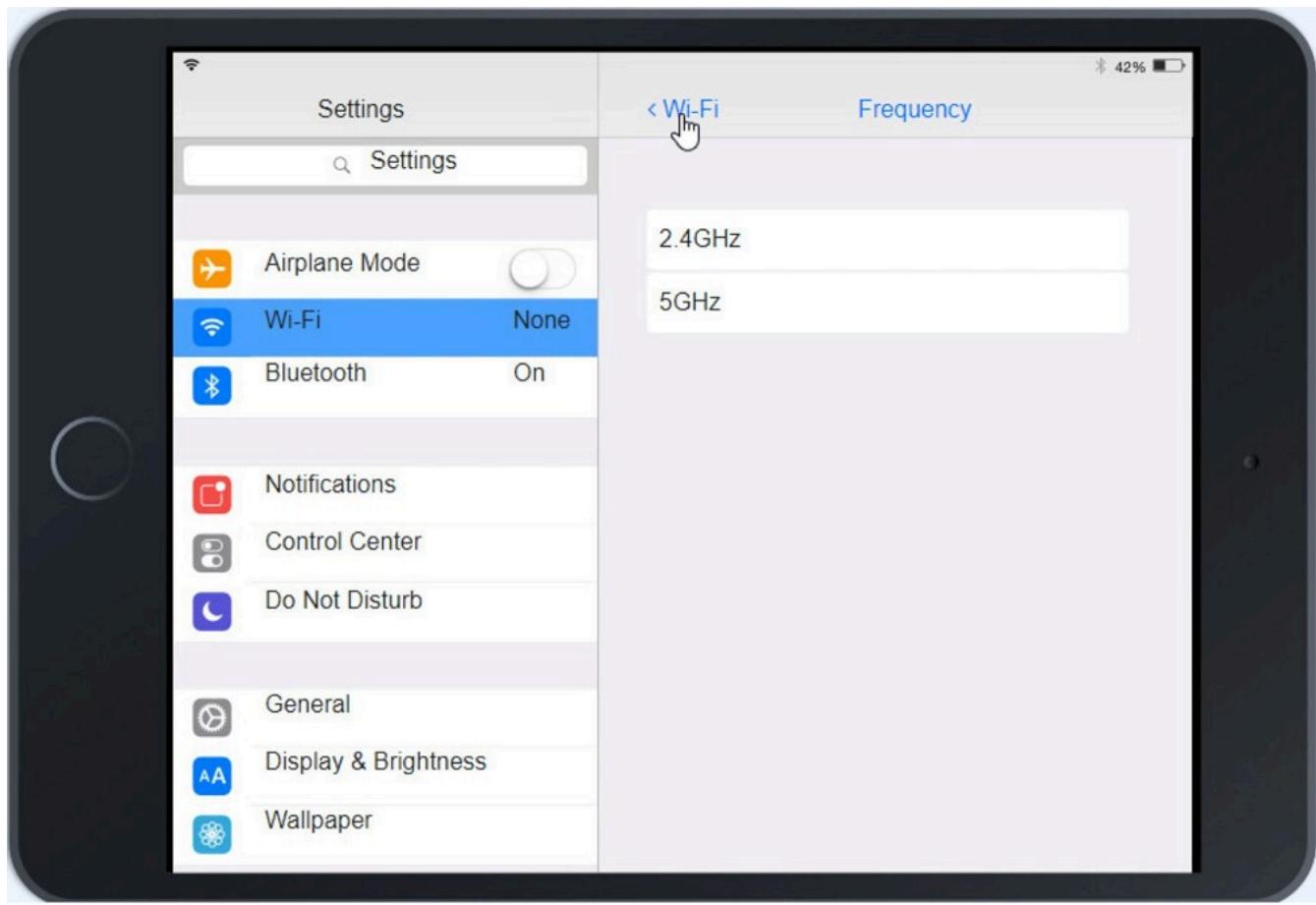
Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.









# Settings

Site

Wireless Networks

Networks

Guest Control

Admins

User Groups

VOIP

## Wireless Networks

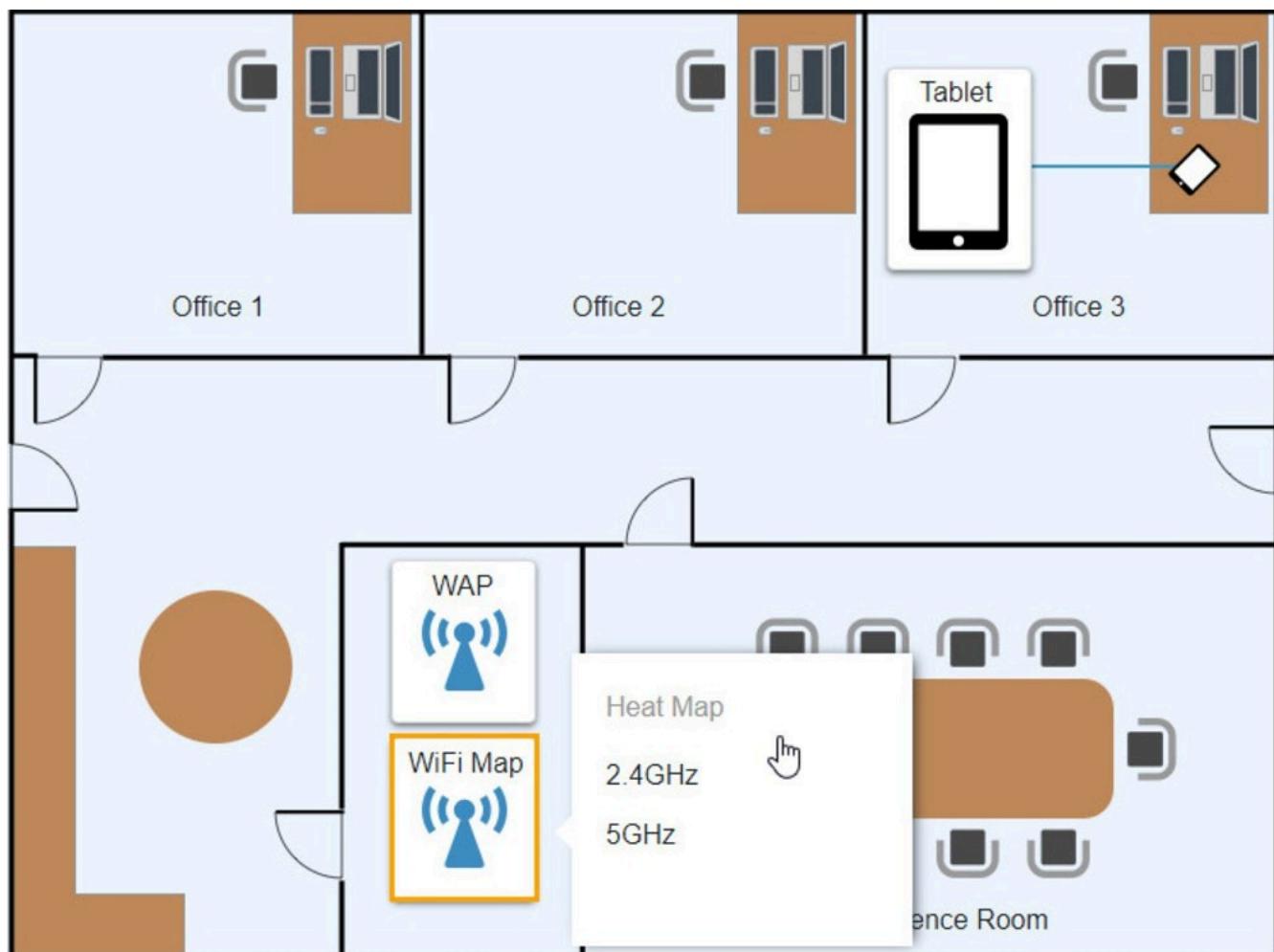
SSID	Frequency	Security	Totally Secure!
CORP	2.4GHz/5GHz	WPA2	Corpsecure1
BYOD	2.4GHz/5GHz ✗	WPA-PSK	TotallySecure!

Create New Wireless Network

Controller

Cloud Access

Maintenance



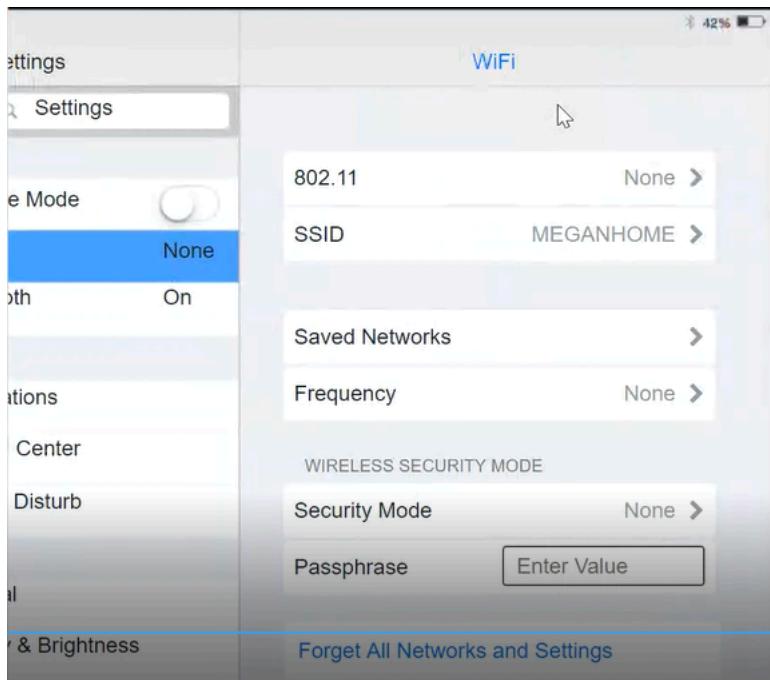
A . See the Explanation below

---

**Answer: A**

---

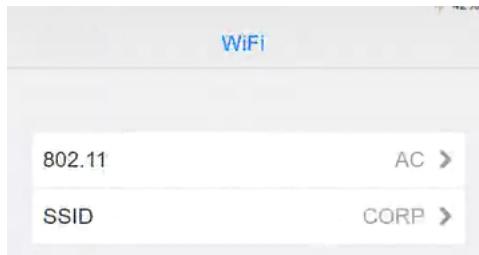
Explanation:



Click on 802.11 and Select ac



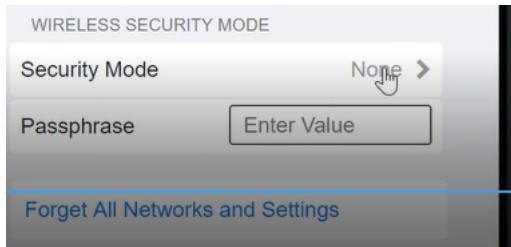
Click on SSID and select CORP



Click on Frequency and select 5GHz



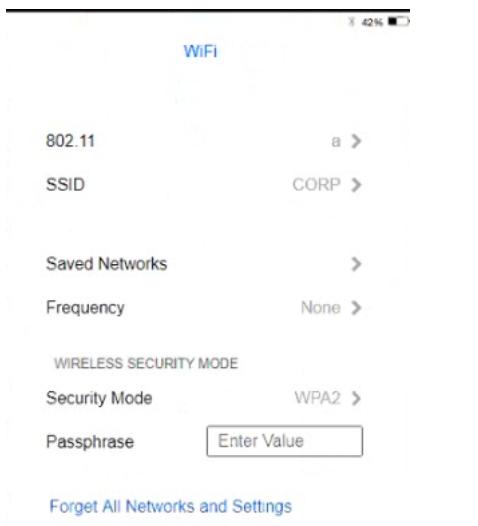
At Wireless Security Mode, Click on Security Mode



Select the WPA2



Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TotallySecret.



---

### **Question: 673**

---

An executive has contacted you through the help-desk chat support about an issue with a mobile device.

Assist the executive to help resolve the issue.

**TEST QUESTION**

An executive has contacted you through the help-desk chat support about an issue with a mobile device.

Assist the executive to help resolve the issue.

**INSTRUCTIONS**  
Select the MOST appropriate statement for each response.  
*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

Telecom.

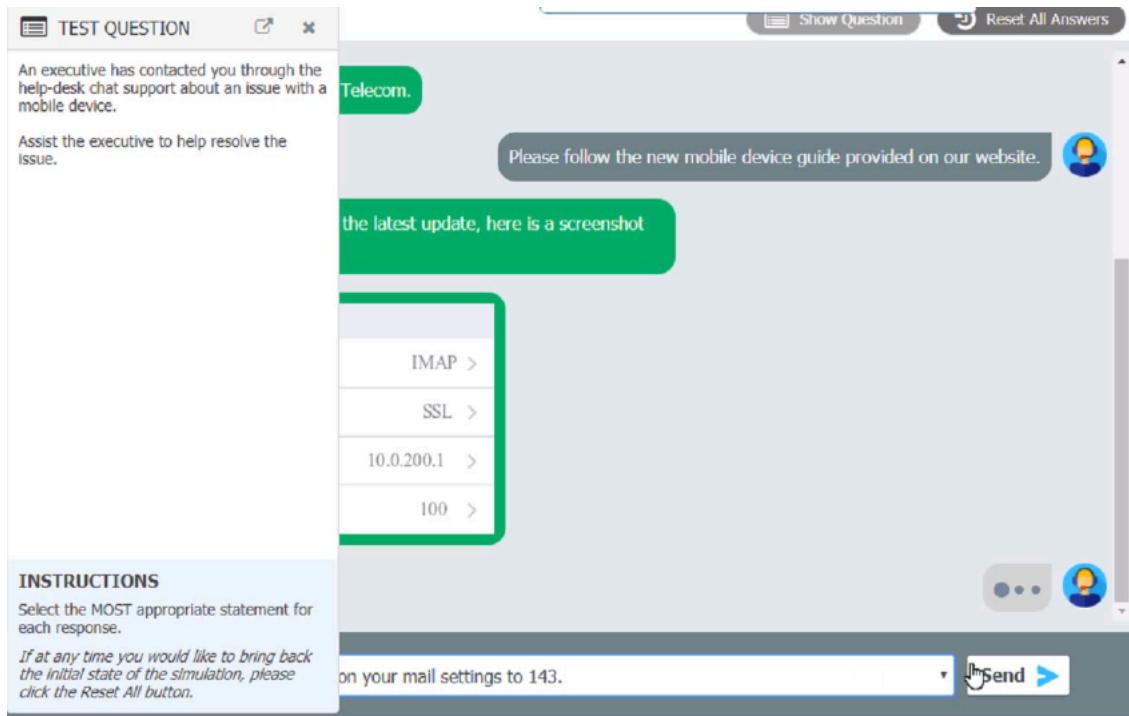
Please follow the new mobile device guide provided on our website.

the latest update, here is a screenshot

IMAP >  
SSL >  
10.0.200.1 >  
100 >

on your mail settings to 143.

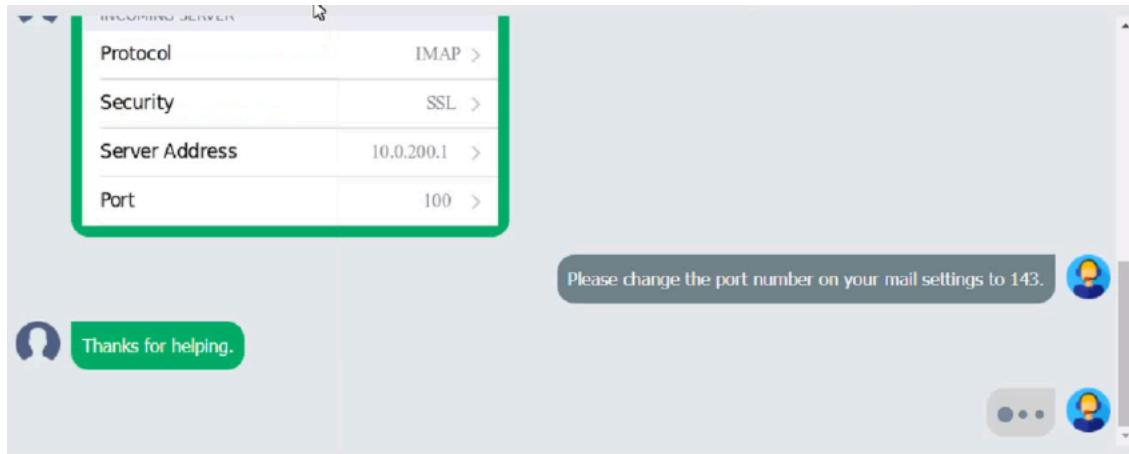
**Send**



Protocol IMAP >  
Security SSL >  
Server Address 10.0.200.1 >  
Port 100 >

Please change the port number on your mail settings to 143.

Thanks for helping.



Which of the following should be done NEXT?

- A . Educate the user on the solution that was performed.
- B . Tell the user to take time to fix it themselves next time.
- C . Close the ticket out.
- D . Send an email to Telecom to inform them of the issue and prevent reoccurrence.

---

**Answer: A**

---

### **Question: 674**

A user reports that a workstation is operating sluggishly. Several other users operate on the same workstation and have reported that the workstation is operating normally. The systems administrator has validated that the workstation functions normally. Which of the following steps should the systems administrator most likely attempt NEXT?

- A . Increase the paging file size
- B . Run the chkdsk command

- C . Rebuild the user's profile
- D . Add more system memory.
- E . Defragment the hard drive.

---

**Answer: C**

---

Explanation:

Since the systems administrator has validated that the workstation functions normally and other users operate on the same workstation without any issues, the next step should be to rebuild the user's profile. This will ensure that any corrupted files or settings are removed and the user's profile is restored to its default state.

---

### **Question: 675**

---

An organization is centralizing support functions and requires the ability to support a remote user's desktop. Which of the following technologies will allow a technician to see the issue along with the user?

- A . RDP
- B . VNC
- C . SSH
- D . VPN

---

**Answer: B**

---

Explanation:

[VNC will allow a technician to see the issue along with the user when an organization is centralizing support functions and requires the ability to support a remote user's desktop1](#)

---

### **Question: 676**

---

A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?

- A . Encryption
- B . Wi-Fi channel
- C . Default passwords
- D . Service set identifier

---

**Answer: C**

---

Explanation:

[the user should change the default passwords first when configuring a new SOHO Wi-Fi router1](#)

---

### **Question: 677**

---

As part of a CYOD policy a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?

- A . Use Settings to access Screensaver settings
- B . Use Settings to access Screen Timeout settings
- C . Use Settings to access General
- D . Use Settings to access Display.

---

**Answer: A**

---

Explanation:

[The systems administrator should use Settings to access Screensaver settings to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity1](#)

---

### **Question: 678**

---

The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

- A . Encryption at rest
- B . Account lockout
- C . Automatic screen lock
- D . Antivirus

---

**Answer: B**

---

Explanation:

[Account lockout would best mitigate the threat of a dictionary attack1](#)

---

### **Question: 679**

---

A technician needs to exclude an application folder from being cataloged by a Windows 10 search. Which of the following utilities should be used?

- A . Privacy
- B . Indexing Options
- C . System

## D . Device Manager

---

**Answer: B**

---

Explanation:

[To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options utility1](#)

---

## Question: 680

---

A technician has spent hours trying to resolve a computer issue for the company's Chief Executive Officer (CEO). The CEO needs the device returned as soon as possible. Which of the following steps should the technician take NEXT?

- A . Continue researching the issue
- B . Repeat the iterative processes
- C . Inform the CEO the repair will take a couple of weeks
- D . Escalate the ticket

---

**Answer: D**

---

Explanation:

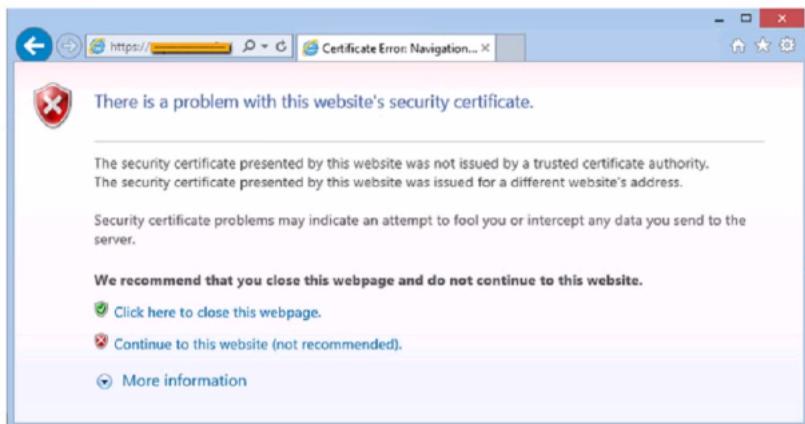
[The technician should escalate the ticket to ensure that the CEO's device is returned as soon as possible1](#)

---

## Question: 681

---

After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:



The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?

- A . Update the browser's CRLs

- B . File a trouble ticket with the bank.
- C . Contact the ISP to report the CFCs concern
- D . Instruct the CFO to exit the browser

---

**Answer: A**

---

Explanation:

The technician should update the browser's CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank's website.

---

### **Question: 682**

---

An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

- A . Encrypt the files
- B . Clone any impacted hard drives
- C . Contact the cyber insurance company
- D . Inform law enforcement

---

**Answer: B**

---

Explanation:

[The incident handler should clone any impacted hard drives to preserve evidence for possible litigation1](#)

---

### **Question: 683**

---

A technician needs to transfer a large number of files over an unreliable connection. The technician should be able to resume the process if the connection is interrupted. Which of the following tools can be used?

- A . afc
- B . ehkdsk
- C . git clone
- C . zobocopy

---

**Answer: A**

---

Explanation:

[The technician should use afc to transfer a large number of files over an unreliable connection and be able to resume the process if the connection is interrupted1](#)

---

### **Question: 684**

---

A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

- A . Configure the network as private
- B . Enable a proxy server
- C . Grant the network administrator role to the user
- D . Create a shortcut to public documents

---

**Answer: A**

---

Explanation:

[The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1](#)

---

### **Question: 685**

---

A technician needs to formal a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

- A . FAT32
- B . ext4
- C . NTFS
- D . exFAT

---

**Answer: C**

---

Explanation:

Since Windows systems support FAT32 and NTFS 'out of the box' and Linux supports a whole range of them including FAT32 and NTFS, it is highly recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS

---

### **Question: 686**

---

A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state but the malware persists. Which of the following would MOST likely resolve the issue?

- A . Quarantining system files

- B . Reimaging the workstation
- C . Encrypting the hard drive
- D . Disabling TLS 1.0 support

---

**Answer: C**

---

Explanation:

[Encrypting the hard drive would most likely resolve the issue1](#)

---

### **Question: 687**

---

A user wants to set up speech recognition on a PC In which of the following Windows Settings tools can the user enable this option?

- A . Language
- B . System
- C . Personalization
- D . Ease of Access

---

**Answer: D**

---

Explanation:

[The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1](#)

Open up ease of access, click on speech, then there is an on and off button for speech recognition.

---

### **Question: 688**

---

Which of the following could be used to implement secure physical access to a data center?

- A . Geofence
- B . Alarm system
- C . Badge reader
- D . Motion sensor

---

**Answer: C**

---

Explanation:

Badge readers are used to implement secure physical access to a data center. They are used to read the identification information on an employee's badge and grant access to the data center if the employee is authorized.2.

This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

---

### Question: 689

---

A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in to the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

- A . Time drift
- B . Dual in-line memory module failure
- C . Application crash
- D . Filesystem errors

---

**Answer: A**

---

Explanation:

The most likely cause of the issue is a "time drift". Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC.12

---

### Question: 690

---

A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?

- A . Disk Cleanup
- B . Group Policy Editor
- C . Disk Management
- D . Resource Monitor

---

**Answer: D**

---

Explanation:

Resource Monitor is a Windows utility that can be used to monitor and analyze the system resources and processes running on a computer. It can be used to identify and troubleshoot any issues that might be causing the computer to run slowly, such as CPU usage, memory usage, disk I/O, and network usage.

---

### Question: 691

---

A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?

- A . resmon.exe
- B . msconfig.exe
- C . dfrgui.exe
- D . msinfo32.exe

---

**Answer: C**

---

Explanation:

[The technician should use dfrgui.exe to defragment the hard drive1](#)

---

### Question: 692

---

A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

- A . Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
- B . Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.
- C . Navigate to the Windows 10 Settings menu, select the Update & Security submenu select Windows Security, select Windows Hello Fingerprint and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
- D . Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

---

**Answer: B**

---

Explanation:

Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates

setup is complete. Windows Hello Fingerprint can be set up by navigating to the Windows 10 Settings menu, selecting the Accounts submenu, selecting Sign in options, and then selecting Windows Hello Fingerprint. The user will then be asked to place a fingerprint on the fingerprint reader repeatedly until Windows indicates that setup is complete. Windows Hello Fingerprint allows the user to log into the laptop using just their fingerprint, providing an additional layer of security.

---

### Question: 693

---

A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access. A technician verifies the user's PC is infected with ransomware. Which of the following should the technician do FIRST?

- A . Scan and remove the malware
- B . Schedule automated malware scans
- C . Quarantine the system
- D . Disable System Restore

---

**Answer: C**

---

Explanation:

[The technician should quarantine the system first1](#)

CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from  
[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

---

### Question: 694

---

A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

- A . MDM
- B . EULA
- C . IRP
- D . AUP

---

**Answer: D**

---

Explanation:

AUP (Acceptable Use Policy) should be updated to reflect this new requirement. The AUP is a document that outlines the acceptable use of technology within an organization. It is a set of rules that employees must follow when using company resources. The AUP should be updated to include a policy on cryptocurrency mining on work desktops.

---

## **Question: 695**

---

A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee. Which of the following methods should the technician use to refresh the laptop?

- A . Internet-based upgrade
- B . Repair installation
- C . Clean install
- D . USB repair
- E . In place upgrade

---

**Answer: C**

---

Explanation:

The desktop specialist should use a clean install to refresh the laptop. A clean install will remove all data and applications from the laptop and install a fresh copy of Windows 10, ensuring that the laptop is ready for the newly hired employee.

---

## **Question: 696**

---

A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?

- A . Right-click the Windows button, then select Run entering shell startup and clicking OK, and then move items one by one to the Recycle Bin
- B . Remark out entries listed HKEY\_LOCAL\_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run
- C . Manually disable all startup tasks currently listed as enabled and reboot checking for issue resolution at startup
- D . Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.

---

**Answer: D**

---

Explanation:

This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab. From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

---

## **Question: 697**

---

A technician is unable to join a Windows 10 laptop to a domain. Which of the following is the MOST likely reason?

- A . The domain's processor compatibility is not met
- B . The laptop has Windows 10 Home installed
- C . The laptop does not have an onboard Ethernet adapter
- D . The Laptop does not have all current Windows updates installed

---

**Answer: B**

---

Explanation:

[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\).pdf](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0).pdf)

---

### **Question: 698**

---

A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?

- A . Operating system updates
- B . Remote wipe
- C . Antivirus
- D . Firewall

---

**Answer: D**

---

Explanation:

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In this scenario, the user is concerned about an installed application transmitting data in the background, so a firewall would be the best solution to address their concern. By installing and configuring a firewall, the user can block unauthorized connections to and from the device, and receive alerts whenever an application tries to access the internet.

---

### **Question: 699**

---

The command `cac cor.pti`

a. `.txt` was issued on a Linux terminal. Which of the following results should be expected?

- A . The contents of the text `comptia.txt` will be replaced with a new blank document
- B . The contents of the text `comptia.txt` would be displayed.
- C . The contents of the text `comptia.txt` would be categorized in alphabetical order.
- D . The contents of the text `comptia.txt` would be copied to another `comptia.txt` file

---

**Answer: B**

---

Explanation:

The command `cac cor.ptia.txt` was issued on a Linux terminal. This command would display the contents of the text file `comptia.txt`.

---

### Question: 700

---

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened while browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?

- A . Shut down the infected computer and swap it with another computer
- B . Investigate what the interface is and what triggered it to pop up
- C . Proceed with initiating a full scan and removal of the viruses using the presented interface
- D . Call the phone number displayed in the interface of the antivirus removal tool

---

**Answer: B**

---

Explanation:

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool12

Shutting down the infected computer and swapping it with another computer is not necessary at this point12

The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

---

### Question: 701

---

During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

- A . set AirDrop so that transfers are only accepted from known contacts
- B . completely disable all wireless systems during the flight
- C . discontinue using iMessage and only use secure communication applications
- D . only allow messages and calls from saved contacts

---

**Answer: A**

---

Explanation:

To best resolve this issue, the executive should set AirDrop so that transfers are only accepted from known contacts (option A). AirDrop is a feature on iOS devices that allows users to share files, photos, and other data between Apple devices. By setting AirDrop so that it only accepts transfers from known contacts, the executive can ensure that unwanted files and photos are not sent to their device. Additionally, the executive should ensure that the AirDrop setting is only enabled when it is necessary, as this will protect their device from any unwanted files and photos.

---

### Question: 702

---

Which of the following provide the BEST way to secure physical access to a data center server room? (Select TWO).

- A . Biometric lock
- B . Badge reader
- C . USB token
- D . Video surveillance
- E . Locking rack
- F . Access control vestibule

---

**Answer: A, B**

---

Explanation:

A biometric lock requires an authorized user to provide a unique biometric identifier, such as a fingerprint, in order to gain access to the server room. A badge reader requires an authorized user to swipe an access card in order to gain access. Both of these methods ensure that only authorized personnel are able to access the server room. Additionally, video surveillance and access control vestibules can be used to further secure the server room. Finally, a locking rack can be used to physically secure the servers, so that they cannot be accessed without the appropriate key.

---

### Question: 703

---

Following the latest Windows update PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?

- A . Network and Sharing Center
- B . Programs and Features
- C . Default Apps
- D . Add or Remove Programs

---

**Answer: C**

---

Explanation:

[Default Apps should be used to ensure all PDF files open in Adobe Reader1](#)

---

## **Question: 704**

---

Which of the following OS types provides a lightweight option for workstations that need an easy-to-use browser-based interface?

- A . FreeBSD
- B . Chrome OS
- C . macOS
- D . Windows

---

**Answer: B**

---

Explanation:

[Chrome OS provides a lightweight option for workstations that need an easy-to-use browser-based interface1](#)

---

## **Question: 705**

---

Upon downloading a new ISO, an administrator is presented with the following string:

59d15a16ce90cBcc97fa7c211b767aB

Which of the following BEST describes the purpose of this string?

- A . XSS verification
- B . AES-256 verification
- C . Hash verification
- D . Digital signature verification

---

**Answer: C**

---

Explanation:

[Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source1](#)

---

## **Question: 706**

---

A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine. The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?

- A . Spyware
- B . Cryptominer
- C . Ransomware

D . Boot sector virus

---

**Answer: B**

---

Explanation:

The type of malware that is most likely to blame for a PC running more slowly than usual and having an extremely high GPU temperature is a "cryptominer". Cryptominers are a type of malware that use the resources of a computer to mine cryptocurrency. This can cause the computer to run more slowly than usual and can cause the GPU temperature to rise. Spyware is a type of malware that is used to spy on a user's activities, but it does not typically cause high GPU temperatures. Ransomware is a type of malware that encrypts a user's files and demands payment to unlock them, but it does not typically cause high GPU temperatures. Boot sector viruses are a type of malware that infects the boot sector of a hard drive, but they do not typically cause high GPU temperatures<sup>12</sup>

---

### **Question: 707**

---

A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?

- A . Run a startup script that removes files by name.
- B . Provide a sample to the antivirus vendor.
- C . Manually check each machine.
- D . Monitor outbound network traffic.

---

**Answer: C**

---

Explanation:

The most effective way to check other machines on the network for this unknown threat is to manually check each machine. This can help to identify any other machines that may be infected with the unknown virus and allow them to be cleaned.

---

### **Question: 708**

---

A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message and no changes have been made within the company. Which of the following has infected the computer?

- A . Cryptominer
- B . Phishing
- C . Ransomware

D . Keylogger

---

**Answer: C**

---

Explanation:

Ransomware is malicious software that encrypts files on a computer, making them inaccessible until a ransom is paid. In this case, the user was able to access the files before without issue, and no changes have been made within the company, so it is likely that the computer was infected with ransomware.

---

### **Question: 709**

---

Which of the following Wi-Fi protocols is the MOST secure?

- A . WPA3
- B . WPA-AES
- C . WEP
- D . WPA-TKIP

---

**Answer: A**

---

Explanation:

[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\).pdf](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0).pdf)

---

### **Question: 710**

---

A department has the following technical requirements for a new application:

Quad Core processor  
250GB of hard drive space  
6GB of RAM  
Touch screens

The company plans to upgrade from a 32-bit Windows OS to a 64-bit OS. Which of the following will the company be able to fully take advantage of after the upgrade?

- A . CPU
- B . Hard drive
- C . RAM
- D . Touch screen

---

**Answer: C**

---

Explanation:

<https://www.makeuseof.com/tag/difference-32-bit-64-bit-windows/>

After upgrading from a 32-bit Windows OS to a 64-bit OS, the company will be able to fully take advantage of the RAM of the computer. This is because a 64-bit operating system is able to use larger amounts of RAM compared to a 32-bit operating system, which may benefit the system's overall performance if it has more than 4GB of RAM installed

---

### Question: 711

---

A user connects a laptop that is running Windows 10 to a docking station with external monitors when working at a desk. The user would like to close the laptop when it is docked, but the user reports it goes to sleep when it is closed. Which of the following is the BEST solution to prevent the laptop from going to sleep when it is closed and on the docking station?

- A . Within the Power Options of the Control Panel utility click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the Plugged In category to Never
- B . Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the On Battery category to Never
- C . Within the Power Options of the Control Panel utility select the option Choose When to Turn Off the Display and select Turn Off the Display under the Plugged In category to Never
- D . Within the Power Options of the Control Panel utility, select the option Choose What Closing the Lid Does and select When I Close the Lid under the Plugged in category to Do Nothing

---

### Answer: D

---

Explanation:

The laptop has an additional option under power and sleep settings that desktops do not have. Switching to do nothing prevents the screen from turning off when closed.

---

### Question: 712

---

A technician is investigating an employee's smartphone that has the following symptoms

- \* The device is hot even when it is not in use.
- \* Applications crash, especially when others are launched
- \* Certain applications, such as GPS, are in portrait mode when they should be in landscape mode

Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

- A . Turn on autorotation
- B . Activate airplane mode.
- C . Close unnecessary applications
- D . Perform a factory reset
- E . Update the device's operating system

F . Reinstall the applications that have crashed.

---

**Answer: A, C**

---

Explanation:

The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscape modes automatically. Closing unnecessary applications can help to free up the device's memory and reduce the device's temperature1

CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives Version 4.0. Retrieved from  
[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0).pdf)

---

### **Question: 713**

---

A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi. When the smartphone is connected to Wi-Fi the user can browse the internet and send and receive email. The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

- A . The smartphone's line was not provisioned with a data plan
- B . The smartphone's SIM card has failed
- C . The smartphone's Bluetooth radio is disabled.
- D . The smartphone has too many applications open

---

**Answer: A**

---

Explanation:

The smartphone's line was not provisioned with a data plan. The user is unable to use any internet-related functions on the smartphone when it is not connected to Wi-Fi because the smartphone's line was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection1

---

### **Question: 714**

---

A technician is configuring a SOHO device. Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same IP address at all times. Which of the following should the technician use?

- A . DHCP reservation
- B . Port forwarding
- C . DNS A record
- D . NAT

---

**Answer: A**

---

Explanation:

The technician should use DHCP reservation to maintain the same IP address for the server at all times. DHCP reservation allows the server to obtain an IP address dynamically from the DHCP server, while ensuring that the same IP address is assigned to the server each time it requests an IP address.

---

### **Question: 715**

---

A company wants to remove information from past users' hard drives in order to reuse the hard drives. Which of the following is the MOST secure method?

- A . Reinstalling Windows
- B . Performing a quick format
- C . Using disk-wiping software
- D . Deleting all files from command-line interface

---

**Answer: C**

---

Explanation:

Using disk-wiping software is the most secure method for removing information from past users' hard drives in order to reuse the hard drives. Disk-wiping software can help to ensure that all data on the hard drive is completely erased and cannot be recovered.

---

### **Question: 716**

---

A user's mobile phone has become sluggish. A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

- A . Prevent a device root
- B . Disable biometric authentication
- C . Require a PIN on the unlock screen
- D . Enable developer mode
- E . Block a third-party application installation
- F . Prevent GPS spoofing

---

**Answer: C, E**

---

Explanation:

To help secure the device against this threat in the future, the administrator should require a PIN on the unlock screen and block a third-party application installation. Requiring a PIN on the unlock screen can help to prevent unauthorized access to the device, while blocking third-party application installation can help to prevent malicious applications from being installed on the device.

---

### Question: 717

---

A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

- A . Utilizing an ESD strap
- B . Disconnecting the computer from the power source
- C . Placing the PSU in an antistatic bag
- D . Ensuring proper ventilation
- E . Removing dust from the ventilation fans
- F . Ensuring equipment is grounded

---

**Answer: A, C**

---

Explanation:

The two safety procedures that would best protect the components in the PC are:

Utilizing an ESD strap

Placing the PSU in an antistatic bag

<https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/>

<https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158>

---

### Question: 718

---

A technician has been tasked with using the fastest and most secure method of logging in to laptops. Which of the following log-in options meets these requirements?

- A . PIN
- B . Username and password
- C . SSO
- D . Fingerprint

---

**Answer: A**

---

Explanation:

This is because a PIN is a fast and secure method of logging in to laptops, and it is more secure than a password because it is not susceptible to keyloggers.

---

### **Question: 719**

---

A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?

- A . WPA2 with TKIP
- B . WPA2 with AES
- C . WPA3 with AES-256
- D . WPA3 with AES-128

---

**Answer: B**

---

Explanation:

This is because WPA2 with AES is the most secure wireless network configuration that is available on a ten-year-old SOHO wireless router.

---

### **Question: 720**

---

A company is issuing smartphones to employees and needs to ensure data is secure if the devices are lost or stolen. Which of the following provides the BEST solution?

- A . Anti-malware
- B . Remote wipe
- C . Locator applications
- D . Screen lock

---

**Answer: B**

---

Explanation:

This is because remote wipe allows the data on the smartphone to be erased remotely, which helps to ensure that sensitive data does not fall into the wrong hands.

---

### **Question: 721**

---

Someone who is fraudulently claiming to be from a reputable bank calls a company employee. Which of the following describes this incident?

- A . Pretexting
- B . Spoofing
- C . Vishing
- D . Scareware

---

**Answer: C**

---

Explanation:

Vishing is a type of social engineering attack where a fraudulent caller impersonates a legitimate entity, such as a bank or financial institution, in order to gain access to sensitive information. The caller will typically use a variety of techniques, such as trying to scare the target or providing false information, in order to get the target to provide the information they are after. Vishing is often used to gain access to usernames, passwords, bank account information, and other sensitive data.

---

### **Question: 722**

---

A call center technician receives a call from a user asking how to update Windows. Which of the following describes what the technician should do?

- A . Have the user consider using an iPad if the user is unable to complete updates
- B . Have the user text the user's password to the technician.
- C . Ask the user to click in the Search field, type Check for Updates, and then press the Enter key
- D . Advise the user to wait for an upcoming, automatic patch

---

**Answer: C**

---

Explanation:

The technician should guide the user to update Windows through the built-in 'Check for Updates' feature. This can be done by having the user click in the Search field, type 'Check for Updates', and then press the Enter key. This will bring up the Windows Update function, which will search for any available updates and give the user the option to install them.

---

### **Question: 723**

---

A company installed a new backup and recovery system. Which of the following types of backups should be completed FIRST?

- A . Full
- B . Non-parity
- C . Differential
- D . Incremental

---

**Answer: A**

---

Explanation:

The type of backup that should be completed FIRST after installing a new backup and recovery system is a full backup. This is because a full backup is a complete backup of all data and is the foundation for all other backups. After a full backup is completed, other types of backups, such as differential and incremental backups, can be performed.

---

**Question: 724**

---

A technician has been tasked with installing a workstation that will be used for point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?

- A . Data-in-transit encryption
- B . File encryption
- C . USB drive encryption
- D . Disk encryption

---

**Answer: D**

---

Explanation:

Disk encryption should be used to secure the workstation in case of theft. Disk encryption can help to protect data on the hard drive by encrypting it so that it cannot be accessed without the correct encryption key.

---

**Question: 725**

---

A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?

- A . Install alternate open-source software in place of the applications with issues
- B . Run both CPU and memory tests to ensure that all hardware functionality is normal
- C . Check for any installed patches and roll them back one at a time until the issue is resolved
- D . Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.

---

**Answer: C**

---

Explanation:

The first step in troubleshooting is to check for any installed patches and roll them back one at a time until the issue is resolved. This can help to identify any patches that may be causing the issue and allow them to be removed.

---

### Question: 726

---

A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

- A . Application updates
- B . Anti-malware software
- C . OS reinstallation
- D . File restore

---

**Answer: C**

---

Explanation:

If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system

<https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html>

---

### Question: 727

---

A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?

- A . Changing channels
- B . Modifying the wireless security
- C . Disabling the SSID broadcast
- D . Changing the access point name

---

**Answer: A**

---

Explanation:

Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

---

### Question: 728

---

An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

- A . All updated software must be tested with alt system types and accessories
- B . Extra technician hours must be budgeted during installation of updates
- C . Network utilization will be significantly increased due to the size of CAD files
- D . Large update and installation files will overload the local hard drives.

---

**Answer: C**

---

Explanation:

The IT manager is most likely to be concerned about network utilization being significantly increased due to the size of CAD files. Backing up all CAD files to the software's cloud server can result in a large amount of data being transferred over the network, which can cause network congestion and slow down other network traffic.

---

### **Question: 729**

---

A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

- A . Avoid distractions
- B . Deal appropriately with customer's confidential material
- C . Adhere to user privacy policy
- D . Set and meet timelines

---

**Answer: A**

---

Explanation:

The technician has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

---

### **Question: 730**

---

Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

- A . Acceptable use
- B . Chain of custody
- C . Security policy
- D . Information management

---

**Answer: B**

---

Explanation:

The aspect of forensic evidence life cycle that must be maintained when dealing with a piece of evidence is chain of custody. This is because chain of custody is the documentation of the movement of evidence from the time it is collected to the time it is presented in court, and it is important to maintain the integrity of the evidence.

---

### **Question: 731**

---

A technician is configuring a new Windows laptop. Corporate policy requires that mobile devices make use of full disk encryption at all times. Which of the following encryption solutions should the technician choose?

- A . Encrypting File System
- B . FileVault
- C . BitLocker
- D . Encrypted LVM

---

**Answer: A**

---

Explanation:

The encryption solution that the technician should choose when configuring a new Windows laptop and corporate policy requires that mobile devices make use of full disk encryption at all times is BitLocker. This is because BitLocker is a full-disk encryption feature that encrypts all data on a hard drive and is included with Windows.

---

### **Question: 732**

---

A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?

- A . Deploy a secondary hard drive with encryption on the appropriate workstation
- B . Configure a hardened SFTP portal for file transfers between file servers
- C . Require files to be individually password protected with unique passwords
- D . Enable BitLocker To Go with a password that meets corporate requirements

---

**Answer: D**

---

Explanation:

The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements. This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data.

---

### Question: 733

---

A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the followings tools should the technician use to accomplish this task?

- A . Consoltf
- B . Disk Utility
- C . Time Machine
- D . FileVault

---

**Answer: B**

---

Explanation:

The technician should use Disk Utility to resize a partition on the internal storage drive of a computer running macOS. Disk Utility is a built-in utility that allows users to manage disks, partitions, and volumes on a Mac. It can be used to resize, create, and delete partitions, as well as to format disks and volumes.

---

### Question: 734

---

The Chief Executive Officer at a bank recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bank's risk? (Select TWO)

- A . Enable multifactor authentication for each support account
- B . Limit remote access to destinations inside the corporate network
- C . Block all support accounts from logging in from foreign countries
- D . Configure a replacement remote-access tool for support cases.
- E . Purchase a password manager for remote-access tool users
- F . Enforce account lockouts after five bad password attempts

---

**Answer: A, F**

---

Explanation:

The best ways to limit the bank's risk are to enable multifactor authentication for each support account and enforce account lockouts after five bad password attempts. Multifactor authentication adds an extra layer of security to the login process, making it more difficult for attackers to gain access to systems. Account lockouts after five bad password attempts can help to prevent brute force attacks by locking out accounts after a certain number of failed login attempts.

---

### **Question: 735**

---

A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

- A . Scan the computer with the company-provided antivirus software
- B . Install a new hard drive and clone the user's drive to it
- C . Deploy an ad-blocking extension to the browser.
- D . Uninstall the company-provided antivirus software
- E . Click the link in the messages to pay for virus removal
- F . Perform a reset on the user's web browser

---

**Answer: C, F**

---

Explanation:

'The user thought the company-provided antivirus software would prevent this issue.'

The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

---

### **Question: 736**

---

A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?

- A . Services
- B . Processes
- C . Performance
- D . Startup

---

**Answer: B**

---

Explanation:

Processes tab in Task Manager would contain the information a technician would use to identify the cause of this issue. The Processes tab in Task Manager displays all the processes running on the computer, including the CPU and memory usage of each process. The technician can use this tab to identify the process that is causing the hard drive activity light to remain lit and the performance degradation1

---

### **Question: 737**

---

A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?

- A . End user acceptance
- B . Perform risk analysis
- C . Communicate to stakeholders
- D . Sandbox testing

---

**Answer: D**

---

Explanation:

The risk analysis should be performed before it's taken to the board. The step after the board approves the change is End User Agreement Reference: [https://www.youtube.com/watch?v=RU77iZxuElA&list=PLG49S3nxzAnna96gzhJrzki4hH\\_mgW4b&index=59](https://www.youtube.com/watch?v=RU77iZxuElA&list=PLG49S3nxzAnna96gzhJrzki4hH_mgW4b&index=59)

---

### **Question: 738**

---

A systems administrator is setting up a Windows computer for a new user. Corporate policy requires a least privilege environment. The user will need to access advanced features and configuration settings for several applications. Which of the following BEST describes the account access level the user will need?

- A . Power user account
- B . Standard account
- C . Guest account
- D . Administrator account

---

**Answer: B**

---

Explanation:

The account access level the user will need to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment is a standard account. This is because a standard account allows the user to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment1.

---

### **Question: 739**

---

Which of the following is the MOST important environmental concern inside a data center?

- A . Battery disposal
- B . Electrostatic discharge mats
- C . Toner disposal
- D . Humidity levels

---

**Answer: D**

---

Explanation:

One of the most important environmental concerns inside a data center is the level of humidity. High levels of humidity can cause condensation, which can result in corrosion of components and other equipment. Low levels of humidity can cause static electricity to build up, potentially leading to electrostatic discharge (ESD) and damage to components. Therefore, it is crucial to maintain a relative humidity range of 40-60% in a data center to protect the equipment and ensure proper operation.

---

### **Question: 740**

---

A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

- A .deb
- B .vbs
- C .exe
- D .app

---

**Answer: D**

---

Explanation:

The file type that the technician will MOST likely use when installing new software on a macOS computer is .app. This is because .app is the file extension for applications on macOS1.

---

### **Question: 741**

---

A technician at a customer site is troubleshooting a laptop A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?

- A . Change the DNS address to 1.1.1.1
- B . Update Group Policy
- C . Add the site to the client's exceptions list
- D . Verify the software license is current.

---

**Answer: C**

---

Explanation:

The technician should add the update site to the client's exceptions list to bypass the proxy. This can be done through the client's web browser settings, where the proxy settings can be configured. By adding the update site to the exceptions list, the client will be able to access the site and download the software update.

---

### Question: 742

---

Once weekly a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows applications?

- A . Install and run Linux and the required application in a PaaS cloud environment
- B . Install and run Linux and the required application as a virtual machine installed under the Windows OS
- C . Use a swappable drive bay for the boot drive and install each OS with applications on its own drive Swap the drives as needed
- D . Set up a dual boot system by selecting the option to install Linux alongside Windows

---

**Answer: B**

---

Explanation:

[The user should install and run Linux and the required application as a virtual machine installed under the Windows OS.This solution would allow for parallel execution of the Linux application and Windows applications2.](#)

[The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS.This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window3.](#)

---

### Question: 743

---

Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?

- A . Home
- B . Pro for Workstations
- C . Enterprise
- D . Pro

---

**Answer: D**

---

Explanation:

The most cost-effective version of Windows 10 that allows remote access through Remote Desktop is Windows 10 Pro. Windows 10 Pro includes Remote Desktop, which allows users to connect to a remote computer and access its desktop, files, and applications. Windows 10 Home does not include Remote Desktop, while Windows 10 Pro for Workstations and Windows 10 Enterprise are more expensive versions of Windows 10 that include additional features for businesses

---

### Question: 744

---

When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

- A . Have the user provide a callback phone number to be added to the ticket
- B . Assign the ticket to the department's power user
- C . Register the ticket with a unique user identifier
- D . Provide the user with a unique ticket number that can be referenced on subsequent calls.

---

**Answer: D**

---

Explanation:

The technician should provide the user with a unique ticket number that can be referenced on subsequent calls to make sure the ticket is associated with the correct user. This is because registering the ticket with a unique user identifier, having the user provide a callback phone number to be added to the ticket, or assigning the ticket to the department's power user will not ensure that the ticket is associated with the correct user.

---

### Question: 745

---

A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?

- A . Remote wipe
- B . Anti-malware
- C . Device encryption
- D . Failed login restrictions

---

**Answer: A**

---

Explanation:

The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device.

---

### **Question: 746**

---

A user is having phone issues after installing a new application that claims to optimize performance. The user downloaded the application directly from the vendor's website and is now experiencing high network utilization and is receiving repeated security warnings. Which of the following should the technician perform FIRST to mitigate the issue?

- A . Reset the phone to factory settings
- B . Uninstall the fraudulent application
- C . Increase the data plan limits
- D . Disable the mobile hotspot.

---

**Answer: B**

---

Explanation:

Installing applications directly from a vendor's website can be risky, as the application may be malicious or fraudulent. Uninstalling the application can help mitigate the issue by removing the source of the problem.

---

### **Question: 747**

---

A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?

- A . Scope of change
- B . Risk level
- C . Rollback plan
- D . End user acceptance

---

**Answer: C**

---

Explanation:

The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

---

### **Question: 748**

---

A technician needs to recommend the best backup method that will mitigate ransomware attacks. Only a few files are regularly modified, however, storage space is a concern. Which of the following backup methods would BEST address these concerns?

- A . Full

- B . Differential
- C . Off-site
- D . Grandfather-father-son

---

**Answer: B**

---

Explanation:

The differential backup method would best address these concerns. Differential backups only back up files that have changed since the last full backup, which means that only a few files would be backed up each time. This would help to mitigate the risk of ransomware attacks, as only a few files would be affected if an attack occurred. Additionally, differential backups require less storage space than full backups.

---

### **Question: 749**

---

A technician receives a ticket indicating the user cannot resolve external web pages. However, specific IP addresses are working. Which of the following does the technician MOST likely need to change on the workstation to resolve the issue?

- A . Default gateway
- B . Host address
- C . Name server
- D . Subnet mask

---

**Answer: A**

---

Explanation:

The technician most likely needs to change the default gateway on the workstation to resolve the issue. The default gateway is the IP address of the router that connects the workstation to the internet, and it is responsible for routing traffic between the workstation and the internet. If the default gateway is incorrect, the workstation will not be able to access external web pages.

---

### **Question: 750**

---

A technician installed a known-good, compatible motherboard on a new laptop. However, the motherboard is not working on the laptop. Which of the following should the technician MOST likely have done to prevent damage?

- A . Removed all jewelry
- B . Completed an inventory of tools before use
- C . Practiced electrical fire safety
- D . Connected a proper ESD strap

---

**Answer: D**

---

#### Explanation:

The technician should have connected a proper ESD strap to prevent damage to the motherboard. ESD (electrostatic discharge) can cause damage to electronic components, and an ESD strap helps to prevent this by grounding the technician and preventing the buildup of static electricity. Removing all jewelry is also a good practice, but it is not the most likely solution to this problem.