Charpter 3 – Quiz

1. Which technology removes direct equipment and maintenance costs from the user for data backups?

- a cloud service
- network attached storage
- a tape
- an external hard drive

Explanation:
The cost of cloud storage commonly depends on the amount of storage space needed. The cloud provider will maintain the equipment and the cloud user will have access to the backup data.

2. A user is surfing the Internet using a laptop from a public WiFi cafe. What should be checked first when the user connects to the public network?

- if the laptop has a master password set to secure the passwords stored in the password manager
- if the laptop requires user authentication for file and media sharing
- if the laptop web browser is operating in private mode
- if the laptop Bluetooth adapter is disabled

Explanation:
When a user connects to a public network, it is important to know if the computer is configured with file and media sharing and that it requires user authentication with encryption.

3.

- Use only an encrypted connection to access websites.
- Move any downloaded files to the recycle bin.
- Reboot the computer after closing the web browser.
- Operate the web browser in private browser mode.

Explanation:
When a computer user browses the web in private mode, the following occurs:
Cookies are disabled.
Temporary Internet files are removed after closing the window.
Browsing history is removed after closing the window.

4. Why do IoT devices pose a greater risk than other computing devices on a network?

- Most IoT devices do not receive frequent firmware updates.
- IoT devices cannot function on an isolated network with only an Internet connection.
- Most IoT devices do not require an Internet connection and are unable to receive new updates.
- IoT devices require unencrypted wireless connections.

Explanation:
IoT devices commonly operate using their original firmware and do not receive updates as frequently as laptops, desktops, and mobile platforms.

5. A consumer would like to print photographs stored on a cloud storage account using a third party online printing service. After successfully logging into the cloud account, the customer is automatically given access to the third party online printing service. What allowed this automatic authentication to occur?

- The user is on an unencrypted network and the password for the cloud storage service is viewable by the online printing service.
- The cloud storage service is an approved application for the online printing service.
- The account information for the cloud storage service was intercepted by a malicious application.
- The password entered by the user for the online printing service is the same as the password used on the cloud storage service.

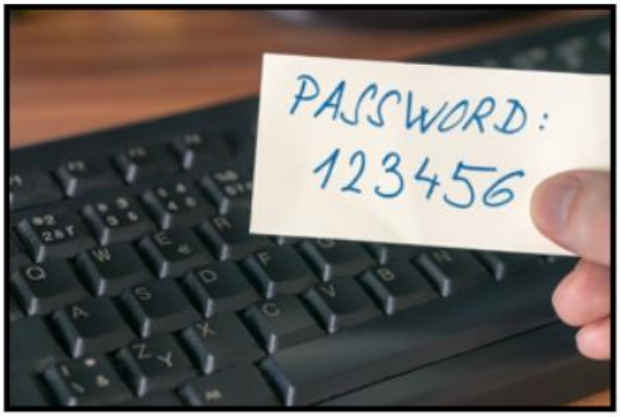
Explanation:
Open Authorization is an open standard protocol that allows end users to access third party applications without exposing the user password.

6. How can a user prevent others from eavesdropping on network traffic when operating a PC on a public Wi-Fi hot spot?

- se WPA2 encryption.
- Connect with a VPN service.
- Disable Bluetooth.
- Create strong and unique passwords.

Explanation:
When a user connects through an encrypted VPN tunnel on a public Wi-Fi network, any data being sent or received from the user will be undecipherable.

7. A network administrator is conducting a training session to office staff on how to create a strong and effective password. Which password would most likely take the longest for a malicious user to guess or break?



- super3secret2password1
- 10characters
- drninjaphd
- mk$$cittykat104#

Explanation:
When choosing a good password:
Do not use dictionary words or names in any languages.
Do not use common misspellings of dictionary words.
Do not use computer names or account names.
If possible use special characters, such as ! @ # $ % ^ & * ( ).
Use a ten character password or more.

8. Which configuration on a wireless router is not considered to be adequate security for a wireless network?

- prevent the broadcast of an SSID
- implement WPA2 encryption
- enabling wireless security
- modify the default SSID and password of a wireless router

Explanation:
A wireless router can be configured to not allow the SSID to be broadcast, but that configuration is not considered to be adequate security for a wireless network

9. What is the best method to prevent Bluetooth from being exploited?

- Always disable Bluetooth when it is not actively used.
- Always use a VPN when connecting with Bluetooth.
- Only use Bluetooth when connecting to a known SSID.
- Only use Bluetooth to connect to another smartphone or tablet.

Explanation:
Bluetooth is a wireless technology that can be exploited by hackers to eavesdrop, establish remote access controls, and distribute malware. A user should keep Bluetooth turned off when not in use.

10. Which type of technology can prevent malicious software from monitoring user activities, collecting personal information, and producing unwanted pop-up ads on a user computer?

- two factor authentication
- firewall
- password manager
- antispyware

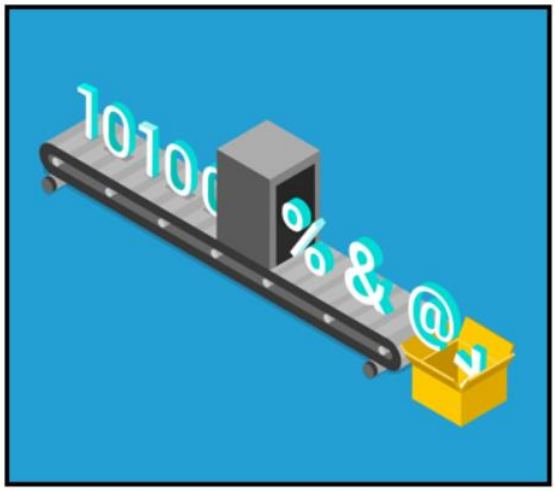
Explanation:
Antispyware software is commonly installed on a user machine to scan and remove malicious spyware software installed on a device.

11. A user is having difficulty remembering passwords for multiple online accounts. What is the best solution for the user to try?

- Share the passwords with the network administrator or computer technician.
- Create a single strong password to be used across all online accounts.
- Save the passwords in a centralized password manager program.
- Write the passwords down and place them out of sight.

Explanation:
A password manager can be used to store and encrypt multiple passwords. A master password can be implemented to protect the password manager software.

12. As data is being stored on a local hard disk, which method would secure the data from unauthorized access?



- a duplicate hard drive copy
- two factor authentication
- data encryption
- deletion of sensitive files

Explanation:
Data encryption is the process of converting data into a form where only a trusted, authorized person with a secret key or password can decrypt the data and access the original form.