16-1Physical and Logical Security

Core 2 Objectives

- 2.1

  Summarize various security measures and their purposes.
- 2.2

  Compare and contrast wireless security protocols and authentication methods.
- 2.3

  Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.
- 2.4

  Explain common social-engineering attacks, threats, and vulnerabilities.
- 2.6

  Given a scenario, configure a workstation to meet best practices for security.
- 3.3

  Given a scenario, use best practice procedures for malware removal.

In this section of the module, you learn about both physical and logical methods of protecting computer resources, including how to control staff access to these resources.

16-1aPhysical Security and Access Controls

Core 2 Objectives

- 2.1

  Summarize various security measures and their purposes.
- 2.6

  Given a scenario, configure a workstation to meet best practices for security.

Physically protecting access to a computer's resources is often seen by security experts as the most important—and most overlooked—form of security. Here are some best practices for physical security used to protect buildings, parking lots, corporate campuses, or other locations:

- **Use security fences and bollards to protect the building.** Your first line of defense to protect valuable data and property is to secure the building through the use of physical barriers such as a **security fence**. A high wire-mesh security fence installed in concrete footings with a secure gate eliminates any possible hiding places and is difficult for someone to climb over or get under, around, or through it. **Bollards**, which are strong metal posts positioned to prevent vehicles from accidentally or intentionally ramming into a protected space, can be used to help protect equipment and the entrance to a building, or to direct traffic. See Figure 16-1.

Figure 16-1

Bollards in front and security fences in the back protect this parcel locker at a London underground station

- **Use an access control vestibule and security guard.** The ultimate in physical security is an **access control vestibule**, also called a **mantrap**, which consists of two doors on either end of a small entryway where the first door must close and/or lock before the second door can open. A separate form of identification might be required for each door, such as a wired or wireless **badge reader** to scan staff badges for the first door (see Figure 16-2) and a fingerprint scanner for the second door. A security guard might also maintain an **entry control roster**, which is a list of people allowed into the restricted area and a log of any approved visitors.

Figure 16-2

A badge reader authenticates a staff badge to allow entry into a secured building

iStock.com/Zinkevych

- **Video surveillance.** A **video surveillance** system includes cameras installed in strategic locations by a government, organization, or school that are monitored for improper activity. A surveillance camera, sometimes called an IP camera, has an IP address to connect it to the local network and is considered a part of the **Internet of Things (IoT)**. It can transmit output to video surveillance software anywhere on the Internet via a wired or wireless connection. Cameras, such as those shown in Figure 16-3, may be fixed or may be able to pan, tilt, or zoom and may have night vision or require proper lighting to work well. A surveillance camera may have a **motion sensor** that can alert security personnel when activity is happening in the vicinity of the camera and turn on recording.

Figure 16-3

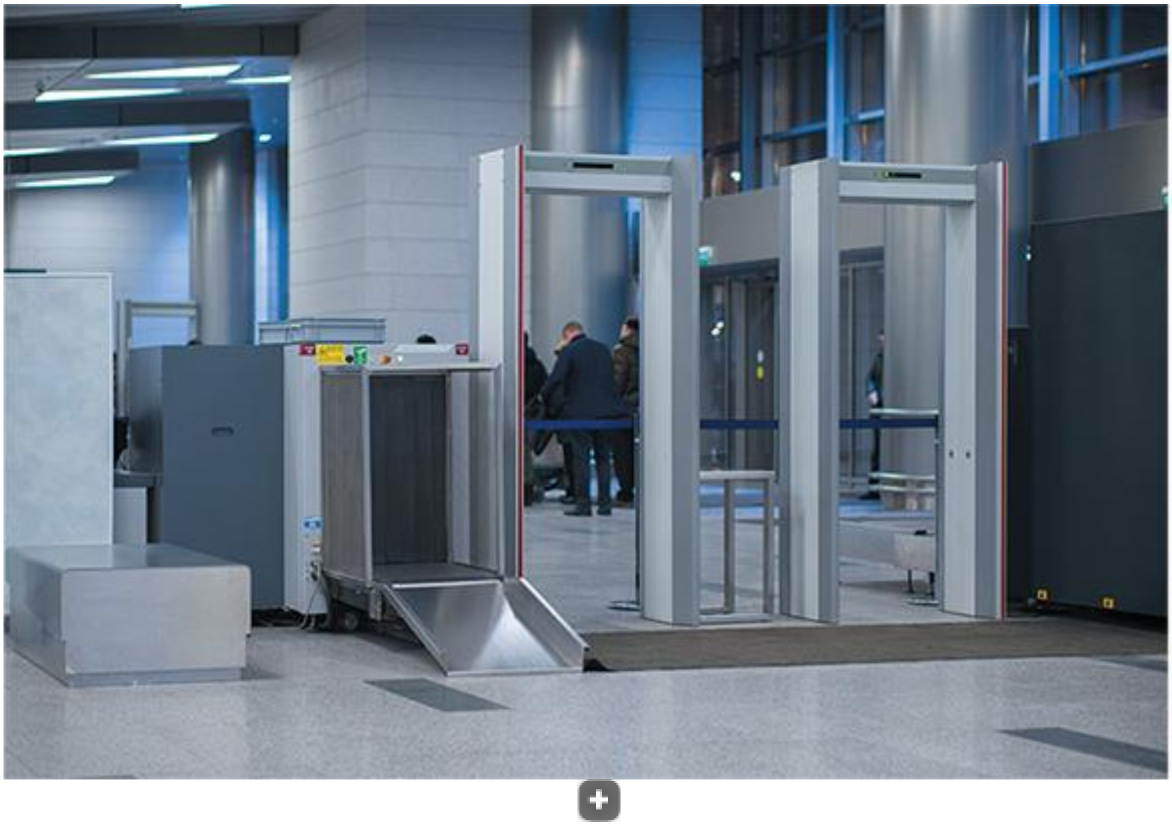
Video surveillance cameras

- The system typically requires large-capacity storage to keep recordings for several days, weeks, or months. Some systems allow real-time monitoring only at one security location or over the Internet, and other systems don't allow real-time monitoring at all; recordings must be viewed after they happen. Important security considerations for a video surveillance system include who in the organization is authorized to view the video and in what capacity the video recordings can be used.

- **Alarm systems.** **Alarm systems** generally use a low-voltage electrical system installed on doors and windows, motion sensors, and perhaps even smoke and carbon monoxide detectors. When alarm sensors detect an interruption in electrical flow or motion, they set off sirens or strobe lights to scare off intruders and wake up sleeping residents, or they may send alerts via text message or phone call to notify security personnel responsible for monitoring the system. An alarm system needs a control panel or other method to stop the alerts when authorized activity is happening.
- **Metal detectors.** A metal detector (see Figure 16-4) uses a **magnetometer**, which detects electromagnetic fields to detect metal objects, such as handguns. Metal detectors are often placed at the front entrance to buildings supervised by security personnel.

Figure 16-4

Metal detectors at entrances to buildings use a magnetometer to detect electromagnetic fields



Andrey Burstein/Shutterstock.com

Andrey Burstein/ Shutterstock.com

Note 1

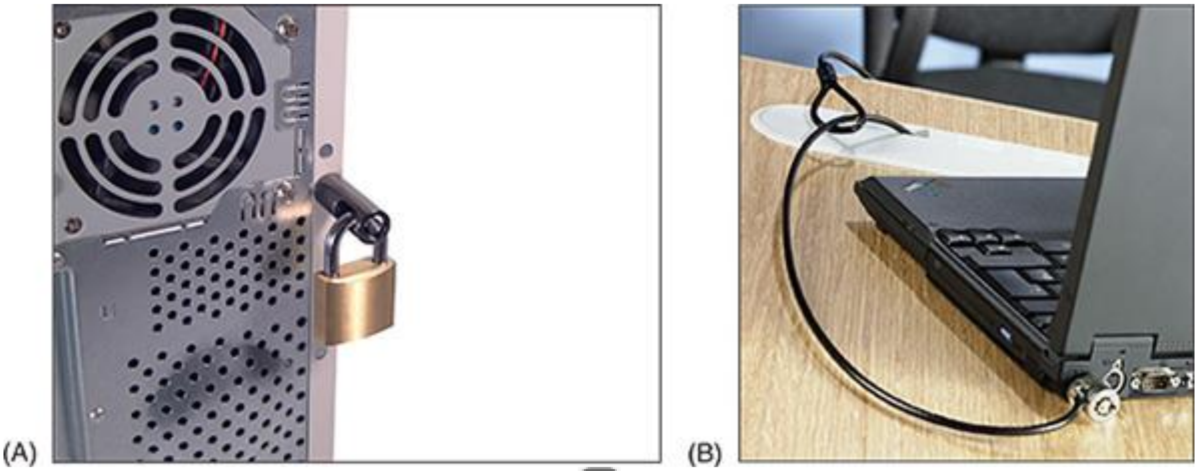
Good security involves multiple layers of defense, which are collectively called **defense in depth**.

Next, we look at physical security focused on protecting data and computers:

- **If the data or equipment is really private, keep it behind a locked door or under lock and key.** You can use all kinds of security methods to encrypt, password-protect, and hide data, but if it really is that important, one obvious thing you can do is to keep the computer behind a locked door. It sounds simple, but it works. You can also store the data on a removable storage device such as an external hard drive, and when you're not using the data, put the drive in a fireproof safe. (And, of course, keep two copies stored in different locations.) Don't forget that printouts of sensitive documents should be kept under lock and key, as well as any passwords you have written down. Door locks and safes come in several types, including keyed locks and combination locks.
- **Equipment locks.** Some computer cases allow you to add a lock so you can physically prevent others from opening the case (see Figure 16-5A). These equipment locks, called **server locks**, might be used on computers that hold corporate data. You can also use a **cable lock**, or **Kensington lock**, to secure a laptop or other computer to a table so someone can't walk away with it (see Figure 16-5B). Most laptops have a security slot on the case to connect the cable lock; this slot is called a **Kensington Security Slot** or K-Slot. Many thefts occur in private offices or hotel rooms, so even if you're not sitting in a public area with your laptop, consider keeping it locked to a nearby table or post. Be sure to choose a cable lock that resists tampering with pliers or cable cutters. Never leave a device out of your sight in a public place.

Figure 16-5

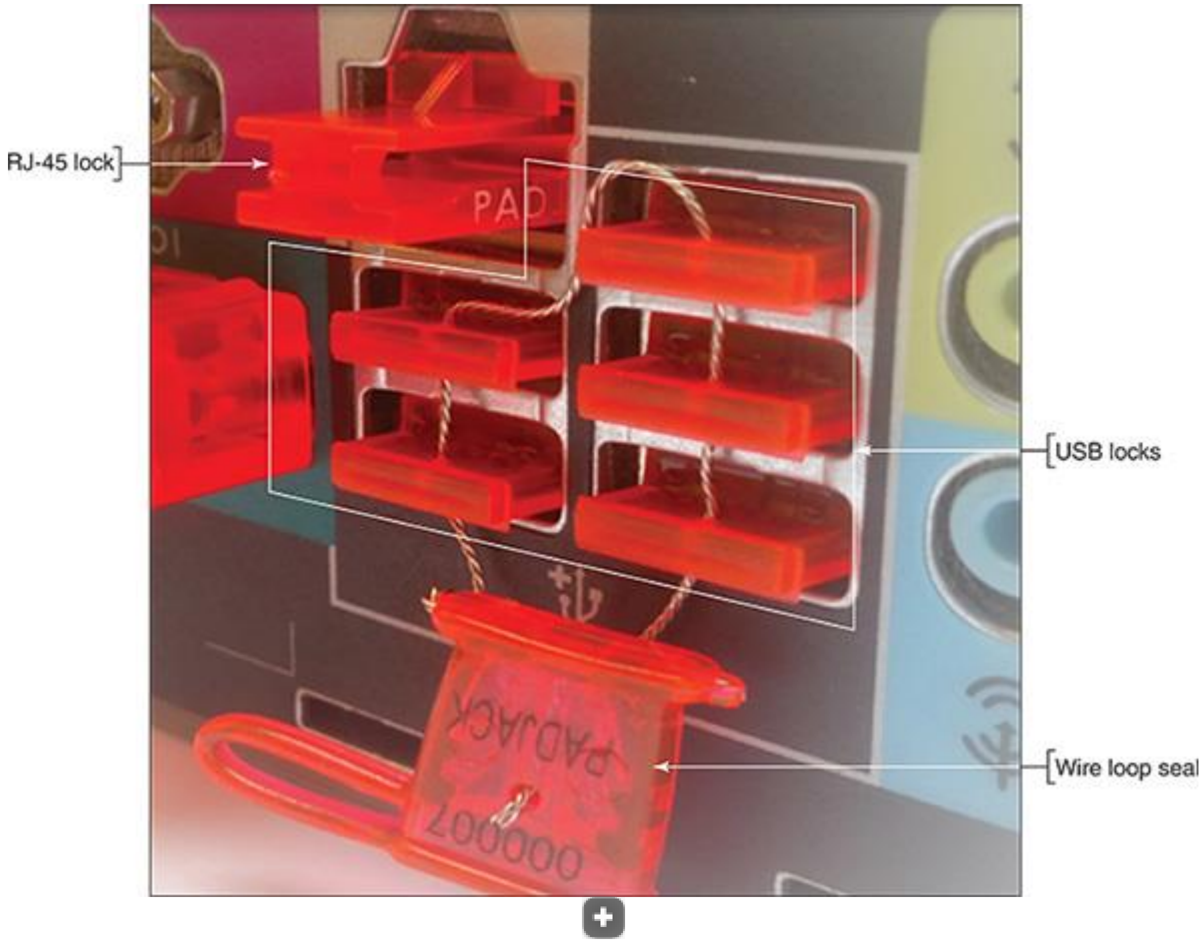
To physically secure a computer, (A) use a computer case lock and key for a desktop to prevent intrusion, or (B) use a cable lock system for a laptop to prevent theft



- **Secure ports with port locks.** Any exposed port on a device, such as an RJ-45 port or a USB port, can be used to access the device and compromise its security. USB ports in particular are security risks due to the ease of uploading malware or downloading sensitive data using a small flash drive carried in someone's pocket. If you can't restrict access to the device itself, you might install a **port lock** to restrict physical access to the exposed ports. The **USB lock** by PadJack, Inc., consists of three pieces, as shown in Figure 16-6. The smaller two pieces are inserted into the USB port, sealed into place with the wire loop, and cannot be removed without damaging the port or destroying the lock. Other port lock designs can lock a cable into the port so it can't be easily removed.

Figure 16-6

These port locks are reusable, but the wire loop seal can be used only once



Source: PadJack.com

- **Use privacy screens.** To keep other people from **shoulder surfing** (secretly peeking at your monitor screen as you work), you can install a **privacy screen**, also called a **privacy filter**, that fits over the screen to prevent it from being read from a wide angle. This is especially useful in tight quarters, such as on an airplane, bus, or subway, or in other exposed locations such as a receptionist’s desk.
- **Install a theft-prevention plate.** As an added precaution, physically mark a computer case or laptop so it can be identified if it is later stolen. You can embed a **theft-prevention plate** into the case and engrave or tattoo your ID information into it. See Figure 16-7. To further help you identify stolen equipment, record serial numbers and model numbers in a safe place separate from the equipment. This information can also be included in an asset management system.

Figure 16-7

The security plate and the tattoo beneath it serve as an asset-management tag and theft-prevention plate

STOP
SECURITY TRACKING OF OFFICE PROPERTY.
Ownership Permanently Monitored
Police Traceable Tattoo Beneath
To Return to Rightful Owner Please Call Toll Free
Within the US: 1-800-473-7867
Outside the US: +800-473-7867-7
or Visit www.stoptheft.com
U S I 8 4 7 0 1

Source: Computer Security

16-1bUsing AAA for Control Access

Core 2 Objectives

- 2.1

  Summarize various security measures and their purposes.
- 2.2

  Compare and contrast wireless security protocols and authentication methods.

When controlling access by staff, vendors, contractors, customers, and other people to secured areas of a building and to protected resources available on the network or Internet, three types of security measures are used: To control access to a resource, a person is first authenticated, and they are also authorized to do only certain things with these resources. In addition, what a person attempts to do or actually does—and the time it takes to do it—can be tracked or logged for future auditing. These three security measures are generally known as **AAA (authenticating, authorizing, and accounting)** or **triple A**. You need to be aware of the following two principles of AAA:

- **A person is authenticated only if they are on the list.** In networking, an **access control list (ACL)** includes which users, devices, or programs have access to a particular resource—such as a printer, folder, or file on a corporate network or computer. Most security measures enforce **multifactor authentication (MFA)**, which requires more than one factor or action to authenticate someone. **Two-factor authentication (2FA)** is most often used, and the two factors normally involve what the user

  - Knows (such as a Windows or Facebook password)
  - Possesses (a token such as a key, smart card, or key fob)
  - Does (such as voice or speech recognition)
  - Is (through the use of biometric data, such as a fingerprint)
- **A person is authorized to do only what their job requires.** Using the **principle of least privilege**, a user is classified to determine the privileges they need to do their jobs. For example, some users need the privilege to sign in to a system remotely, and others do not. Generally, when a new employee begins work, that employee's job description, with exceptions approved by their supervisor, determine what privileges the employee needs to perform their job. You, as the support technician, would be responsible to make sure the user account assigned to the employee has these privileges and no more.

Hard and Soft Tokens

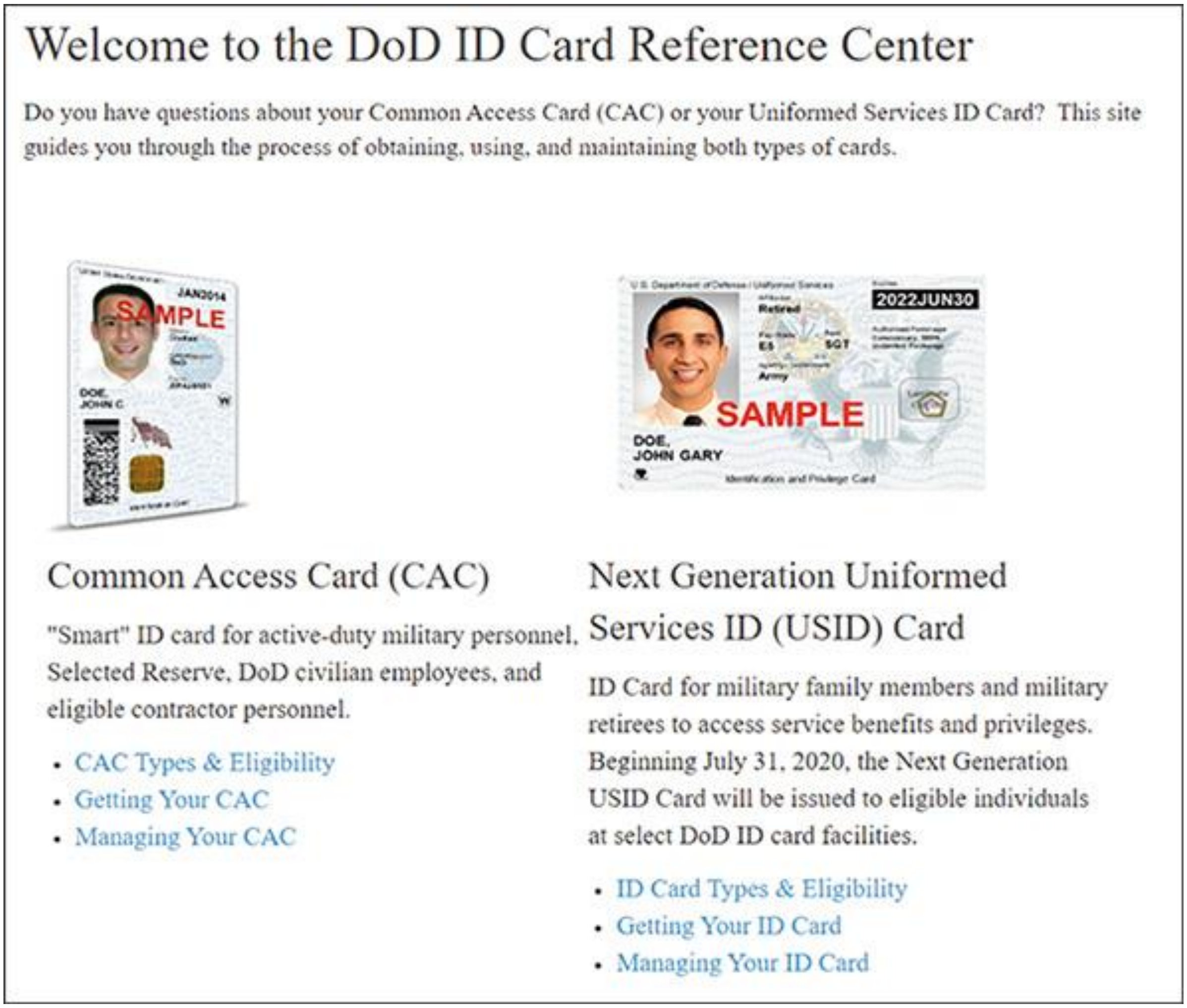
Tokens used to restrict who can access a secured physical location, such as entrance into a building or to a network, might be a **hard token** (a physical device you possess) or a **soft token** (data you can retrieve):

- **Key.** It may sound old-fashioned, but a simple key is a hard token that can open a locked door. In the security world, it's important to know who has been assigned a given key and which locks the key can open.
- **Smart card.** A **smart card** used as a hard token has an embedded microprocessor usually installed on the card under a small gold plate. For example, most current credit cards have a gold plate and microprocessor and are smart cards, as opposed to earlier credit cards that used only a magnetic strip with no internal processor. The microprocessor contains information that is read by a **smart card reader** or badge reader when the device is inserted into the reader or transmitted wirelessly. Refer back to Figure 16-2.

  A smart card that is able to authenticate the reader is called a command access card (CAC). This **mutual authentication** occurs when authentication goes in both directions at the same time and both entities confirm the identity of the other. A CAC used by the Department of Defense can include personal data such as the user's name, digital signature, fingerprints, photo, department, date of birth, and even medical records. See Figure 16-8.

Figure 16-8

A webpage by the DoD shows the smart cards used for mutual authentication and transfer of data



Welcome to the DoD ID Card Reference Center

Do you have questions about your Common Access Card (CAC) or your Uniformed Services ID Card? This site guides you through the process of obtaining, using, and maintaining both types of cards.

Common Access Card (CAC)

"Smart" ID card for active-duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel.

- CAC Types & Eligibility
- Getting Your CAC
- Managing Your CAC

Next Generation Uniformed Services ID (USID) Card

ID Card for military family members and military retirees to access service benefits and privileges. Beginning July 31, 2020, the Next Generation USID Card will be issued to eligible individuals at select DoD ID card facilities.

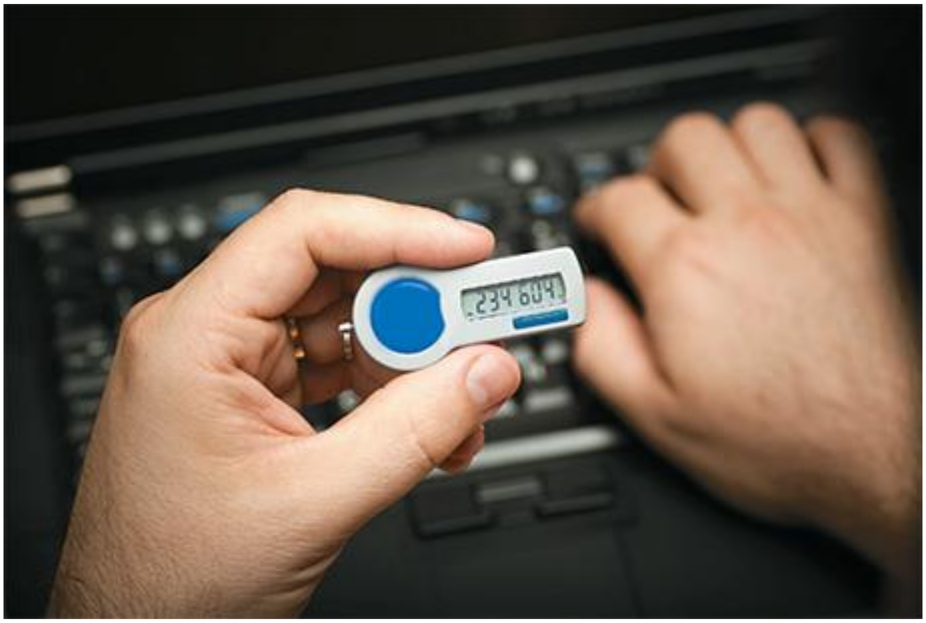
- ID Card Types & Eligibility
- Getting Your ID Card
- Managing Your ID Card

Source: DoD Common Access Card

- Because a smart card contains a microprocessor and data, it’s considered both a hard token and a soft token.
- **Key fob.** A **key fob** is a token that fits conveniently on a keychain, such as the one shown in Figure 16-9. When a user signs in to the network, they must enter the number on the key fob, which changes every 60 seconds and is synchronized with the network authentication service. Entering the number proves that the user has the key fob in hand. Because the device doesn’t actually make physical contact with the system, it is called a contactless token or disconnected token.

Figure 16-9

A security token such as this key fob is used to authenticate a user gaining access to a secured network



Source: iStock.com/David Clark

- **Biometrics.** **Biometric locks** require special input called **biometric data** to identify a person via a retina scanner, fingerprint scanner, or palm print scanner. Figure 16-10 shows a fingerprint scanner. Many mobile devices, such as iPads and some laptops, have fingerprint scanners built in.

Figure 16-10

This access control device accepts typed code, fingerprint, or smart card input

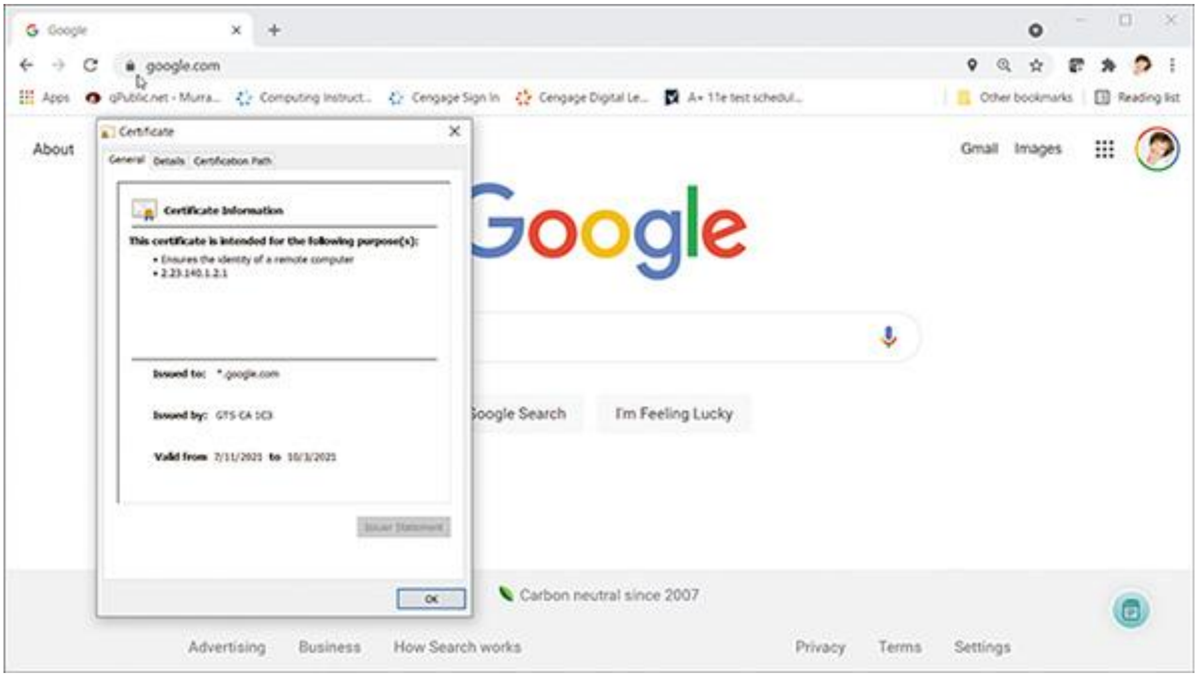
Source: iStock.com/Viiwwee

- **Digital certificates.** Think of a **digital certificate** as a digital signature that proves a person or entity, such as a web server, is who they say they are. It's a small file that holds information about the identity of the person or entity. In addition, a public encryption key is used to prove the certificate is legitimate; it's similar to a notary verifying that a signature is legitimate. The digital certificate and public encryption key are assigned by a **Certificate Authority (CA)** that has confirmed your identity in a separate process. VeriSign (verisign.com), GlobalSign (globalsign.com), and Let's Encrypt (letsencrypt.org) are three well-known CAs. You purchase a digital certificate from a CA and then install it on your desktop, laptop, or other computing device; in some cases, you can install it on a smart card or flash drive that you can use on any computer.

  Digital certificates are used to authenticate individuals (such as to digitally sign and encrypt email or to connect to a corporate network via a VPN), software (Windows can require that device drivers be digitally signed), or server applications (many web servers are digitally signed). For example, to see a web server's digital certificate, navigate to the webpage in your browser, click the lock icon, and then click Certificate. Figure 16-11 shows information about the *.*google.com* certificate.

Figure 16-11

The *google.com* website certificate includes the IP address of the web server



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- 2.23.140.1.2.1

Issued to: *.google.com

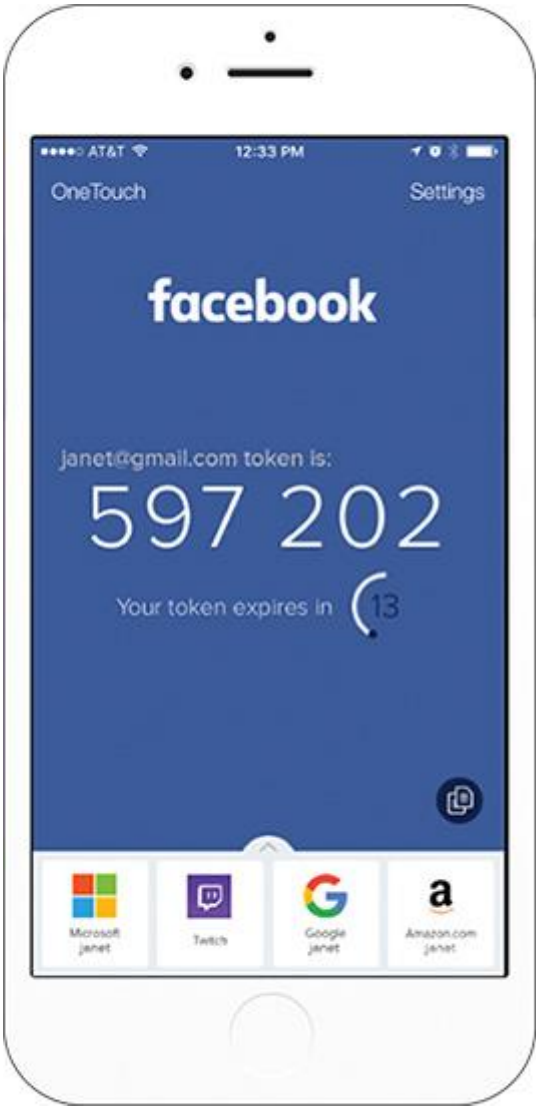
Issued by: GTS CA 1C3

Valid from 7/11/2021 to 10/3/2021

- **Authenticator apps.** An **authenticator app**, sometimes called a software token app, is installed on your smartphone or other computing device to provide a counter or number generator similar to that provided by a key fob for one factor in multifactor authentication. The app is synchronized with the same calculations on the server so the app and the server expect the same number at the same time. Software token providers for 2FA include Google Authenticator (google.com), Twilio Authy (authy.com), and LastPass Authenticator (lastpass.com/auth). Many online accounts—such as banking accounts, Facebook, Google, and Amazon—can be set to use 2FA and software tokens. For example, the Authy app by Twilio can be used to require 2FA to sign in to Facebook (see Figure 16-12).

Figure 16-12

When you sign in to your account, Facebook requests the token generated by the 2FA app



janet@gmail.com token is:

597 202

Your token expires in 13

Source: Twilio, Inc.

In general, to set up 2FA with an online account, you would do the following:

1. Sign up for and configure the 2FA service with a 2FA provider such as Twilio. You'll need to download and install its authenticator app to your phone or computer.
2. Enable 2FA with a Facebook, Google, banking, or other account you want to secure.
3. Configure the account to use the 2FA service.
4. Now, each time you sign in to the account, you must provide your password and the number generated by the authenticator app.

Note 2

A common use of multifactor authentication (MFA) is sending a confirmation code by text to your smartphone using a phone number the server already has on file. The problem with this method is that text messages are sent to a phone using the **short message service (SMS)** protocol, which is not encrypted and can be hacked. The same goes for voice calls used for MFA, which can also be hacked because voice is not encrypted. Rather than text or voice MFA, for better security, use an authenticator app.

Email Filtering

One more security feature that controls what someone is authorized to do on the job is email filtering. Most email providers offer **email filtering** to filter out suspicious messages based on databases of known scams, spammers, and malware. Corporations might route incoming and outgoing email through a proxy server for filtering with the following goals in mind:

- Incoming email is inspected for scams or spam that might trick an employee into introducing malware into the corporate network.
- Outgoing email from employees might be filtered for inappropriate content. This lawful interception is intended to verify that an employee is complying with privacy laws (for example, laws that protect confidential medical records) and is not accidentally or intentionally leaking corporate data and secrets. Email filtering software used in this way is an example of **data loss prevention (DLP)** software, which helps protect against leaking corporate data.

16-1cSocial Engineering and User Education

Core 2 Objectives

- 2.3

  Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.
- 2.4

  Explain common social-engineering attacks, threats, and vulnerabilities.
- 2.6

  Given a scenario, configure a workstation to meet best practices for security.
- 3.3

  Given a scenario, use best practice procedures for malware removal.

Generally speaking, people are the weakest link in setting up security in a computer environment. That's because people can often be tricked into giving out private information and allowing access to secure systems. Even with all the news and hype about identity theft and criminal websites, it's amazing how well they still work. Many users naively download a funny screen saver, open an email attachment, or enter credit card information on a website without regard to security. In the IT arena, **social engineering** is the practice of tricking people into giving out private information or allowing unsafe programs into a network or computer.

A good support technician is aware of the criminal practices used and is able to teach users how to recognize and avoid this mischief. Many organizations routinely offer **security awareness training**, also known as **anti-phishing training,** to its employees to help them recognize common threats and social engineering situations. In this part of the module, you learn about several of these need-to-know practices.

Protect Passwords

It's important for users to understand they need to protect their passwords, personally identifiable information (PII), and other sensitive data. Train users to not send this type of data over email or carelessly leave it in sight on a desk or printer. Always shred documents containing sensitive data before putting them in the trash. Sanitize a device before disposing of it (you learn about ways to sanitize devices later in this module). Other ways to protect passwords include the following:

- Never give out your passwords to anyone, not even a supervisor or tech support person who calls and asks for it.
- Don't store your passwords on a computer unless you use company-approved password vault software (for example, KeePass or LastPass). Some organizations even forbid employees from writing down their passwords.
- Don't use the same password on more than one computer, network, application, or website.

You learn more about protecting passwords in later modules.

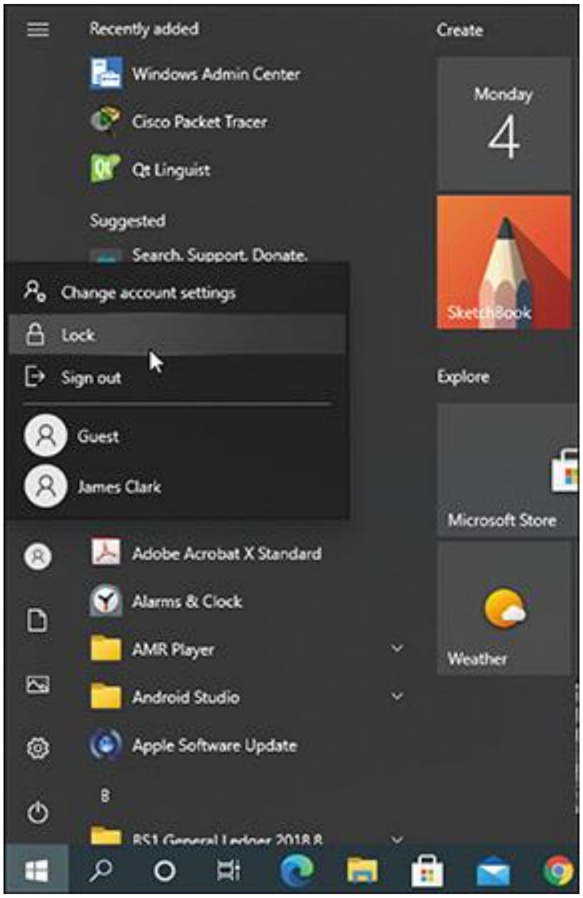
Prevent Tailgating

Users need to be on the alert for **tailgating**, which is when an unauthorized person follows an employee through a secured entrance to a room or building or continues a Windows session after the authorized user has stepped away. To help prevent tailgating a Windows session, a user needs to do the following:

- **Sign out of or lock the workstation.** Make it a habit to sign out of or lock the workstation when not in use. To do that in Windows, click **Start**, click the account icon, and click either **Sign out** or **Lock**. To use the keyboard shortcut to lock the workstation, press **Windows+L**. See Figure 16-13. The difference between the two is that when you sign out, all your apps are closed and your Windows session ends. When you lock the workstation, your session stays open, and your apps continue to run until you enter your password to continue your session.

Figure 16-13

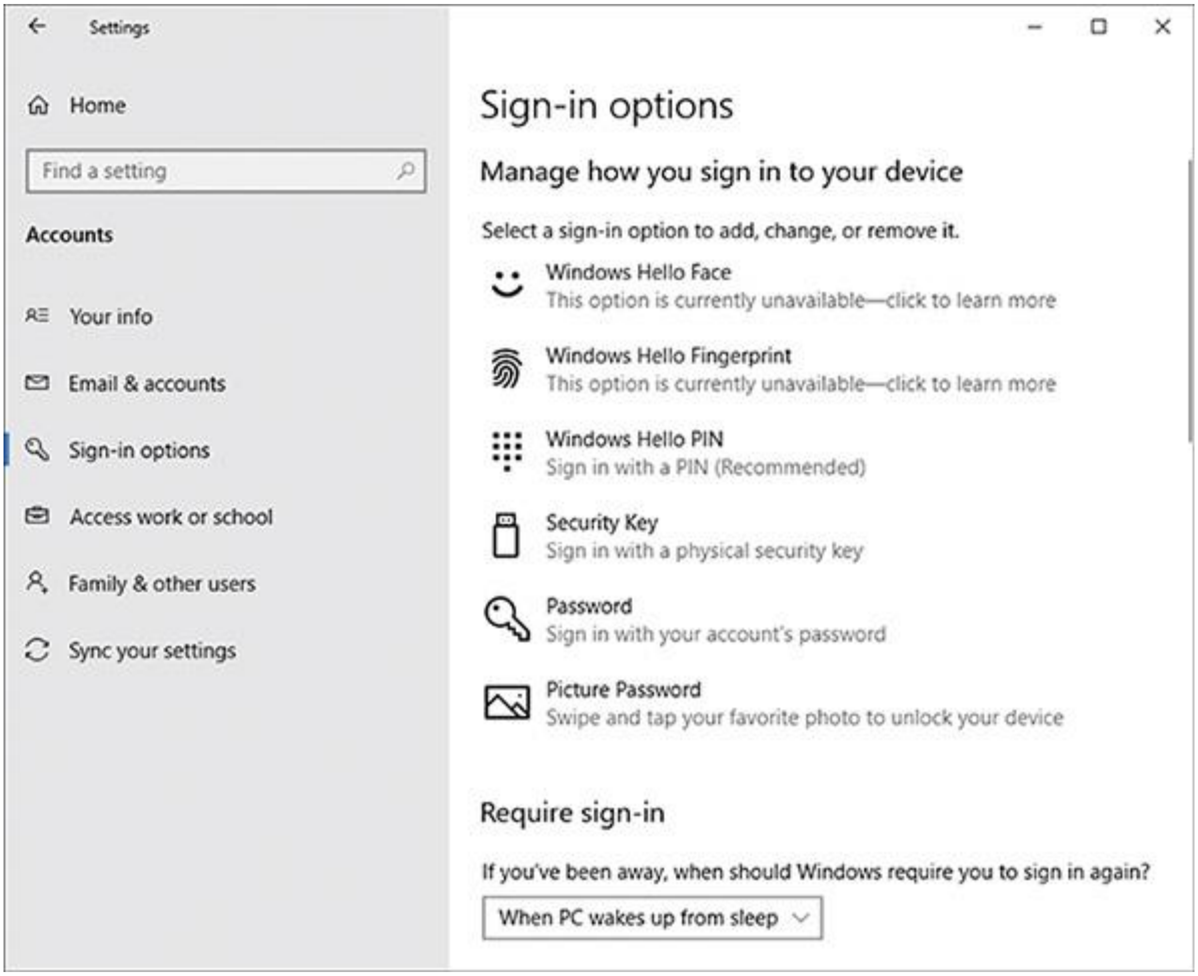
Sign out or lock Windows when the workstation is not in use



- **Screensaver lock.** After a period of inactivity, a computer normally displays a screensaver and goes into sleep mode until a key is pressed to wake it up. A **screensaver lock** locks the computer before it goes to sleep and requires a password to unlock it before restoring the user session. To configure a screensaver lock in Windows, in the Settings app, select **Accounts** and then **Sign-in options**. See Figure 16-14. Verify **When PC wakes up from sleep** is selected.

Figure 16-14

Require signing in each time your computer wakes from sleep mode



Sign-in options

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Windows Hello Face
This option is currently unavailable—click to learn more

Windows Hello Fingerprint
This option is currently unavailable—click to learn more

Windows Hello PIN
Sign in with a PIN (Recommended)

Security Key
Sign in with a physical security key

Password
Sign in with your account's password

Picture Password
Swipe and tap your favorite photo to unlock your device

Require sign-in

If you've been away, when should Windows require you to sign in again?

When PC wakes up from sleep

Common Social Engineering Techniques

Users need to be aware of these social engineering techniques and understand how to resist hackers trying to gain access to networks, computers, and sensitive data:

- **Dumpster diving and impersonation.** **Dumpster diving** is looking for useful information in someone's trash to help create a convincing **impersonation** of an individual or company to aid in a malicious attack. Even something that might appear harmless, such as an organizational chart, can help a thief create a convincing email hoax message. For best security, shred all papers and printouts before recycling, and educate users about the importance of shredding.
- **Phishing, whaling, and vishing.** **Phishing** (pronounced "fishing") is a type of identity theft in which the sender of an **email hoax** scams you into responding with personal data about yourself. A phishing attack that targets a high-profile employee, such as the CEO or CFO, is called **whaling**. **Vishing** is phishing with voice and is a phone call scam that tries to lure you into giving out personal information.
- **Spear phishing and spoofing.** Even more plausible than phishing is **spear phishing**, where an email appears to come from companies

you already do business with. The scam artist baits you by asking you to verify personal data on your bank account, ISP account, credit card account, or something of that nature. Often a convincing impersonation of an individual or company tricks you into responding to the email or clicking a link in the email message, which takes you to an official-looking site complete with corporate or bank logos, where you are asked to enter your user ID and password to enter the site. This tactic is called **spoofing**, which means the scammer makes both the email and website look like the real thing. An email message might contain a link that leads to a malicious script. If you think an email is legitimate, be on the safe side and don't click the link. To keep a script from running, type the website's home page into your browser address bar and navigate to the relevant page on the website.

Good sites to help you debunk a virus hoax or email hoax are the following:

- snopes.com by Snopes Media Group Inc.
- breakthechain.org by John R. Ratliff
- securelist.com by Kaspersky Lab

Don't forward an email hoax. If you get a hoax from a person you know, do us all a favor and send that person some of the preceding links!

✔ Exam Tip

The A+ Core 2 exam expects you to recognize and distinguish among examples of social engineering situations that might compromise security, such as shoulder surfing, tailgating, dumpster diving, impersonations, phishing, whaling, vishing, spoofing, and insider threats.

Next, we turn our attention to dealing with malware. As an IT support technician, you will most certainly be called on to handle it.

16-2Dealing with Malicious Software on Personal Computers

Core 2 Objectives

- 1.3

  Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
- 2.3

  Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.
- 2.4

  Explain common social-engineering attacks, threats, and vulnerabilities.

- 2.5

  Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
- 3.2

  Given a scenario, troubleshoot common personal computer (PC) security issues.
- 3.3

  Given a scenario, use best practice procedures for malware removal.

Malicious software, also called **malware**, is any unwanted program that is intended for harm and is transmitted to your computer without your knowledge. **Grayware** is any annoying and unwanted program that might or might not intend harm—for example, adware that produces all those unwanted pop-up ads. In this section of the module, you learn about the different types of malware and grayware, what to do to clean up an infected system, and how to protect a system from infection.

16-2aWhat Are We Up Against?

Core 2 Objective

- 2.3

  Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.

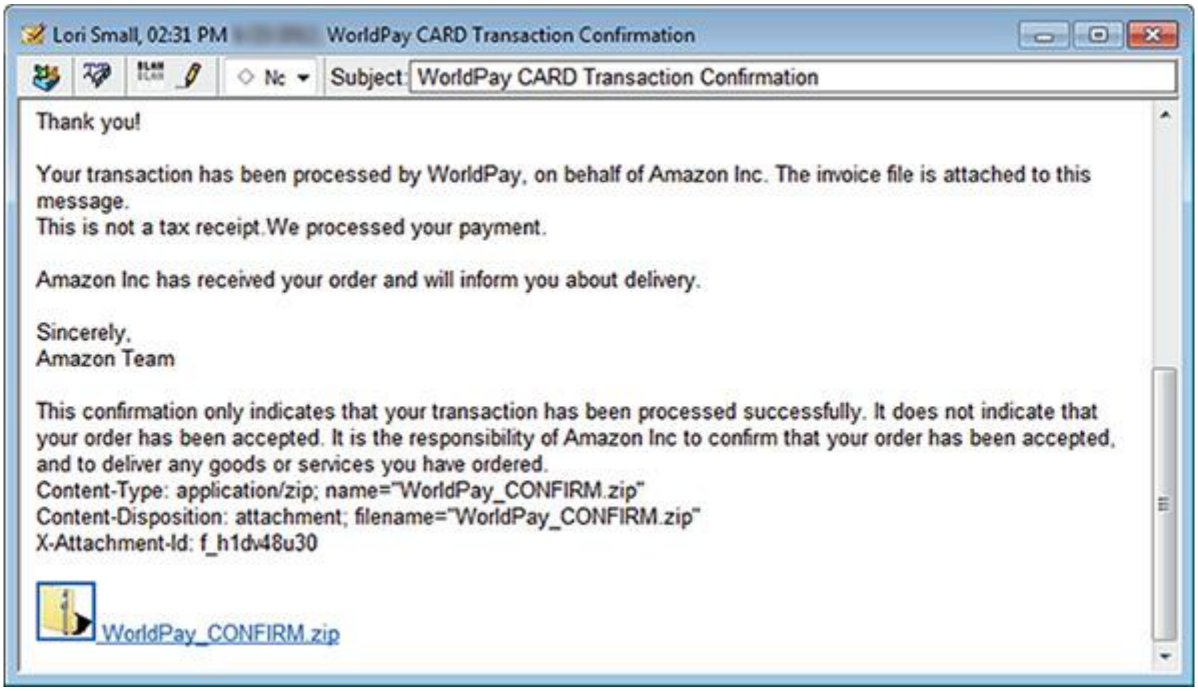
You need to know your enemy! According to metadata from anti-malware developers, more than 560,000 new malware programs are detected daily. Different categories of malware and scamming techniques are listed next:

- **Viruses.** A **virus** is a program that replicates by attaching itself to other programs. The infected program must be executed for a virus to run. The program might be an application, a macro in a document, a Windows system file, or a boot loader program.
- **Spyware.** **Spyware** spies on you to collect personal information that it transmits over the Internet to web-hosting sites. An example of spyware is a **keylogger** that tracks all your keystrokes and can be used to steal your identity, credit card numbers, Social Security number, bank information, passwords, email addresses, and so forth.
- **Worms.** A **worm** is a program that copies itself throughout a network or the Internet without a host program. A worm creates problems by overloading the network as it replicates and can even hijack or install a server program such as a web server.
- **Trojans.** A **Trojan** does not need a host program to work; rather, it substitutes itself for a legitimate program. In most cases, a user launches it thinking they are launching a legitimate program. A Trojan

is often embedded in the files of legitimate software that is downloaded from an untrustworthy website, or a user is tricked into opening an email attachment (see Figure 16-15).

Figure 16-15

By opening this email attachment, a user is likely to introduce a Trojan into the system



Lori Small, 02:31 PM [redacted] WorldPay CARD Transaction Confirmation

Subject: WorldPay CARD Transaction Confirmation

Thank you!

Your transaction has been processed by WorldPay, on behalf of Amazon Inc. The invoice file is attached to this message.
This is not a tax receipt.We processed your payment.

Amazon Inc has received your order and will inform you about delivery.

Sincerely,
Amazon Team

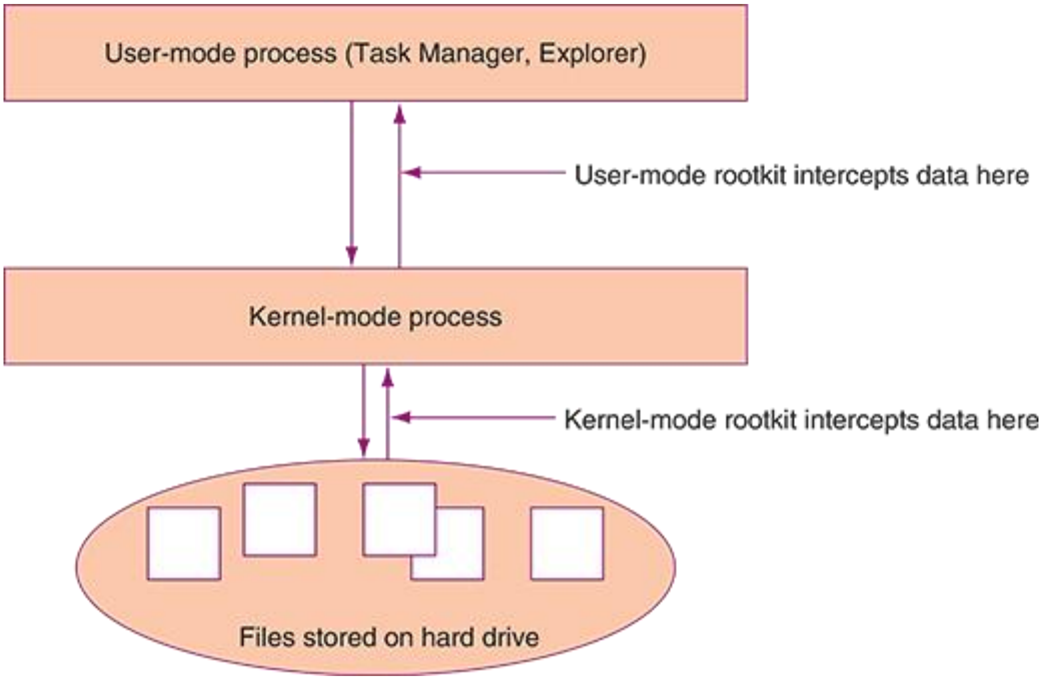
This confirmation only indicates that your transaction has been processed successfully. It does not indicate that your order has been accepted. It is the responsibility of Amazon Inc to confirm that your order has been accepted, and to deliver any goods or services you have ordered.
Content-Type: application/zip; name="WorldPay_CONFIRM.zip"
Content-Disposition: attachment; filename="WorldPay_CONFIRM.zip"
X-Attachment-Id: f_h1dv48u30

WorldPay_CONFIRM.zip

- **Rootkits.** A **rootkit** loads itself before the OS boot is complete. It can hide in boot managers, boot loader programs, or kernel mode device drivers. UEFI secure boot is especially designed to catch rootkits that launch during the boot. Because a rootkit is already loaded when most anti-malware software loads, it is sometimes overlooked by the software. A rootkit can hide folders that contain software it has installed, cause Windows Task Manager to display a different name for its process, hide registry keys, and can operate in user mode or kernel mode. This last trick helps it remain undetected (see Figure 16-16).

Figure 16-16

A rootkit can run in user mode or kernel mode


User-mode process (Task Manager, Explorer)
User-mode rootkit intercepts data here
Kernel-mode process
Kernel-mode rootkit intercepts data here
Files stored on hard drive

- A rootkit running in user mode intercepts the API calls between the time the API retrieves the data and when it is displayed in a window. A rootkit running in kernel mode actually interferes with the Windows kernel and substitutes its own information in place of the raw data read by the Windows kernel. Because most anti-malware software to one degree or another relies on operating system tools and components to work, the rootkit is not detected or cannot be deleted if the OS tools themselves are infected.

! Caution

If anti-malware software reports that a rootkit is present but cannot delete it, the best solution is to immediately disconnect the computer from the network (if you have not already done so), back up your important data, format your hard drive, and reinstall the OS.

- **Boot sector virus.** A **boot sector virus** infects the first sector on a MBR (Master Boot Record) hard drive and can infect the partition table in that sector. The virus works by replacing the program in the first sector, which is used to boot the system. The infection usually happens when you boot a computer with bootable media, such as a USB flash drive, that is infected. To remove a boot sector virus, you'll need antivirus software that runs in a preinstallation environment before the OS launches. Boot sector viruses are not as common as they once were because hard drives use the newer GPT partitioning system rather than the more vulnerable MBR system and also because modern BIOS/UEFI is designed to detect and stop these viruses.

Note 3

Although malicious software is designed to do varying degrees of damage to data and software, it does not damage computer hardware. However, when partition table information is destroyed on a hard drive, the drive can appear to be physically damaged.

- **Ransomware. Ransomware** holds your computer system hostage until you pay money. For example, the infamous CryptoLocker Trojan program was embedded in email attachments and was known to work on Windows, Android, and even some iOS systems. When the user clicked the attachment, the program encrypted the computer's personal files. If the user didn't pay within a 24-hour period, all the files were lost. Many users who did not have backups of their data chose to pay the ransom. A computer infected with ransomware can infect all computers on the network and even cloud servers to which the computer connects.

Caution

The best defense against ransomware is to keep backups of data file versions in a location that is not accessible from Windows File Explorer or macOS Finder. A ransomware attack can infect any storage device connected or mapped to your computer, and a single layer of data file backups might be replaced with the encrypted files before you're able to clean your computer and restore the backed-up data. Use a backup method that retains multiple file versions (indefinitely, if possible) and that is not directly accessible from your computer. Many cloud backup services meet these requirements, such as Carbonite (carbonite.com), Backblaze (backblaze.com), and IDrive (idrive.com). After a ransomware attack, you can wipe the computer, reinstall software from original sources, and restore unaffected file versions from your online backups.

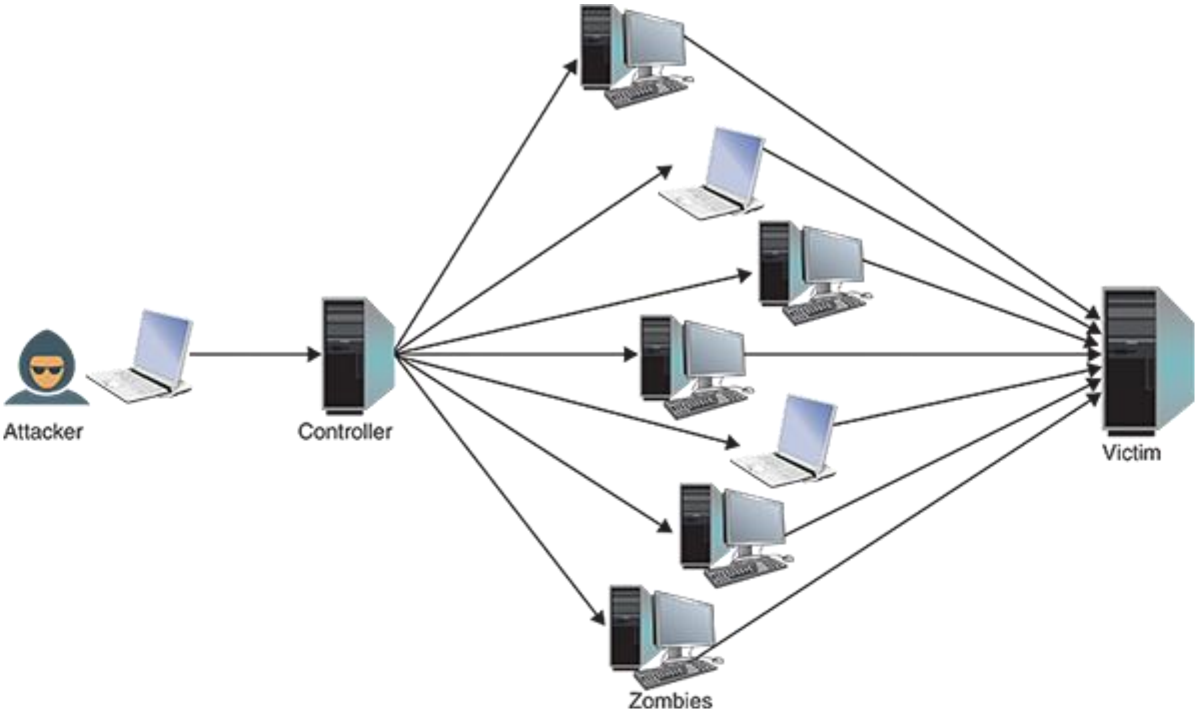
- **On-path attack.** In an **on-path attack**, also called a **man-in-the-middle attack**, the attacker intercepts communication between two parties and reads and/or alters the content of messages. The attacker can impersonate a legitimate website, network, FTP site, or person in a chat session. For example, a user might connect to a fraudulent Wi-Fi hotspot, called an **evil twin**, thinking it's a legitimate hotspot, and attempt to start a chat session with a business associate. The attacker pretends to be the business associate and continues the chat with the intention of obtaining private information. The best protection against on-path attacks is to use digital certificates to identify a person or service before transmitting sensitive information. Sometimes an evil twin hotspot exists only to steal passwords. When connecting to a public hotspot, especially one that requires signing in, be sure the hotspot is legitimate.
- **Zero-day attack.** A **zero-day attack** can happen in two ways: A hacker discovers a security hole in software that is unknown to the developer of the software, or a hacker takes advantage of a recently reported gap in software security before users apply patches released by the developer. The race is on for the vendor to provide a patch to

the software and for users to apply those patches before hackers have even one day to use the hole to infect systems and steal user data. Microsoft normally publishes security patches on the second Tuesday of each month (known as patch Tuesday), but sometimes releases patches off schedule so hackers have less time to attack customers.

- **Denial of service.** A **denial-of-service (DoS)** attack overwhelms a computer or network with requests or traffic until new connections can no longer be accepted. A **distributed denial-of-service (DDoS)** attack happens when multiple computers are involved in the attack. As shown in Figure 16-17, DDoS attacks are sometimes performed by zombies and botnets, which are described next.

Figure 16-17

A DDoS attack might use a network of zombies called a botnet



- **Zombies and botnets.** A **zombie** is a computer that has been hacked, and the hacker is using the computer to run repetitive software in the background without the knowledge of its user. For example, the zombie might be email spamming or performing DDoS attacks. A hacker might build an entire network of zombies, which is called a **botnet** (a network of robots). The CryptoLocker Trojan program was distributed by a botnet and ultimately isolated when the botnet was taken down. **Cryptojacking** is a type of zombie attack that installs crypto mining software to run mining operations. **Crypto miner** software validates cryptocurrency transactions, and these transactions are linked to the ongoing chains of transactions called blockchains.

- **Dictionary attack.** A **dictionary attack** can be used to crack a password by trying words in a dictionary. Password cracker software might combine a **brute force attack** (systematically trying every possible combination of letters, numbers, and symbols) with a dictionary attack to guess the password. A dictionary attack is usually more efficient than using brute force.
- **Rainbow tables.** A **rainbow table** contains a long list of plaintext passwords, just as users would enter, and the password hash list (after it is encrypted). Organizations store only hashed passwords and not plaintext passwords. When hackers obtain a stolen list of hashed passwords, they can compare this list with those in their rainbow tables to find a match. When two hashed passwords match, they can use the plaintext password in the rainbow table to sign in to the system, impersonating the user.

  Rainbow tables make cracking passwords faster than dictionary cracking or brute force cracking. The best defenses against rainbow table attacks are for an organization to use the very best hashing techniques to encrypt their passwords and to add extra characters to the password hash (called salting the passwords).

✔ Exam Tip

The A+ Core 2 exam might give you a scenario that requires you to identify, detect, remove, or prevent viruses, Trojans, spyware, keyloggers, ransomware, rootkits, boot sector viruses, on-path attacks, zero-day attacks, DoS/DDoS attacks, crypto mining software, and dictionary attacks.

16-2bWhat Makes Us the Most Vulnerable?

Core 2 Objective

- 2.4

Explain common social-engineering attacks, threats, and vulnerabilities.

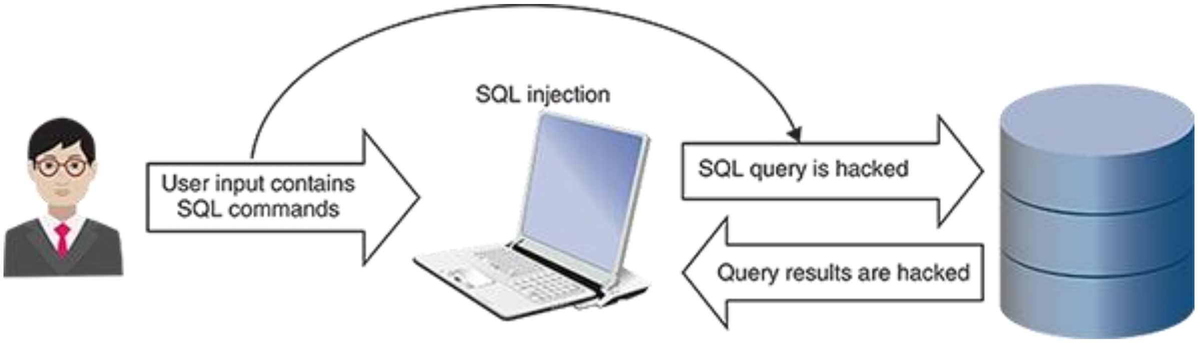
Listed next are some reasons systems are the most vulnerable to attacks:

- **Noncompliant systems.** A system administrator needs techniques in place to routinely scan BYOD and corporate-owned smartphones, tablets, laptops, desktops, and servers for **noncompliant systems** that violate security best practices, such as an OS that is not kept updated or anti-malware software that is not up to date or not even installed. One software suite of products designed to manage user devices in an organization is Microsoft Endpoint Manager. One component of this suite is Configuration Manager, which can scan devices for noncompliance. BYODs are particularly susceptible to noncompliance because a corporation generally has less control over a user-owned device than one owned by the corporation and assigned to the user.

- **Unprotected and unpatched systems.** Personal devices that are not managed by a corporation are especially vulnerable when the OS is not kept up to date with all available patches and anti-malware is not running in real time or kept up to date. For a workstation or laptop system, it's also important that firewalls are set for maximum protection, especially when the computer is connected to a public network.
- **End-of-life OS.** If the OS has reached the end of its life cycle, the developer no longer provides security patches, making the OS vulnerable to attack. It's time to upgrade the OS to a current edition.
- **Structured Query Language (SQL) injections.** **Structured Query Language (SQL)** is a popular scripting and programming language designed primarily to query databases. SQL programmers can carelessly create vulnerabilities in their software, making it possible for hackers to inject their own code in a query to the database and retrieve data they are not authorized to access. An **SQL injection** happens when part of a user's typed text is used to construct a query, and a hacker familiar with SQL uses text that actually changes the query (see Figure 16-18). The programmer can prevent SQL injections by creating queries that only use prepared text rather than untrusted user text. Another solution is to allow untrusted text in a query only if the text can be found in a whitelist of approved text.

Figure 16-18

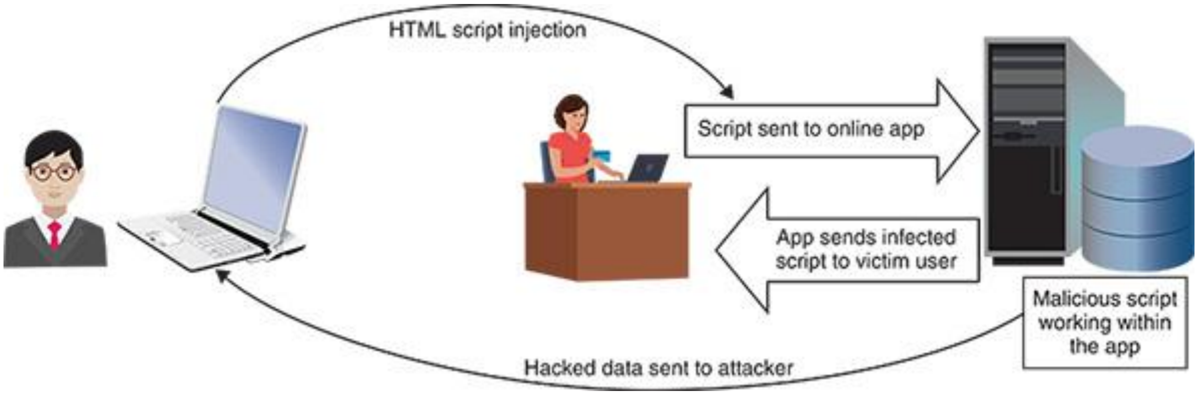
An SQL injection alters an SQL query to change the output from the query



- **Cross-site scripting (XSS).** **Cross-site scripting (XSS)** happens when an attacker sends a malicious script to an online application, and the application unknowingly sends the script to an unsuspecting user's browser, which executes the script under the user's credentials. See Figure 16-19. This script might instruct the online app to send sensitive data to the hacker or even give the hacker control of the app. An online app is vulnerable to this type of injection attack if the app's developer does not carefully test each data entry point in the app to ensure that scripts cannot be accepted as user input.

Figure 16-19

A cross-site scripting (XSS) attack


HTML script injection
Script sent to online app
App sends infected script to victim user
Malicious script working within the app
Hacked data sent to attacker

Note 4

SQL and HTML scripts are vulnerable to injection attacks because the scripts can be a combination of text and commands, and text can be interpreted as commands by simply inserting a few key characters in the right place. You learn more about scripting in the module, "Linux and Scripting."

- **Insider threats.** Employees and others who have legitimate access to the network and data can be a threat if they are careless or negligent and accidentally leak data or fall victim to a social engineering attack. In addition, malicious insiders might intentionally steal data or do other damage.
- **Lack of user education.** Cybint (cybintsolutions.com) reports that 95% of online attacks are caused by human error. Lack of user education about how to avoid attacks makes systems especially vulnerable.

16-2c Step-By-Step Attack Plan

Core 2 Objective

- 3.3

  Given a scenario, use best practice procedures for malware removal.

This section provides a step-by-step attack plan to clean up an infected system. We use **anti-malware software**, also called **antivirus software**, to remove all types of general malware, including viruses, spyware, worms, and rootkits. Then we'll use some Windows tools to check out the system, making sure all remnants of malware have been removed and the system is in tip-top order.

Caution

If a system is highly infected and will later hold sensitive data, a fresh start might be in order. In fact, Microsoft recommends reinstalling Windows as the safest way to deal with highly infected systems. If you have recent backups of data, format the hard drive, reinstall or reimage Windows, and restore data from backups.

If you don't have recent backups for a Windows 10/11 system, you can try a repair installation or a Windows reset without losing user data. In the module, "Troubleshooting Windows Startup," you learned about all of these options to reinstall Windows.

As you work your way through the steps described next to remediate an infected system, at any point in the process, you might realize the system is highly infected and the best course of action is to stop remediating the system and to simply reinstall the OS.

16-2dStep 1: Identifying and Researching Malware Symptoms

Core 2 Objectives

- 1.3

  Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
- 3.2

  Given a scenario, troubleshoot common personal computer (PC) security issues.
- 3.3

  Given a scenario, use best practice procedures for malware removal.

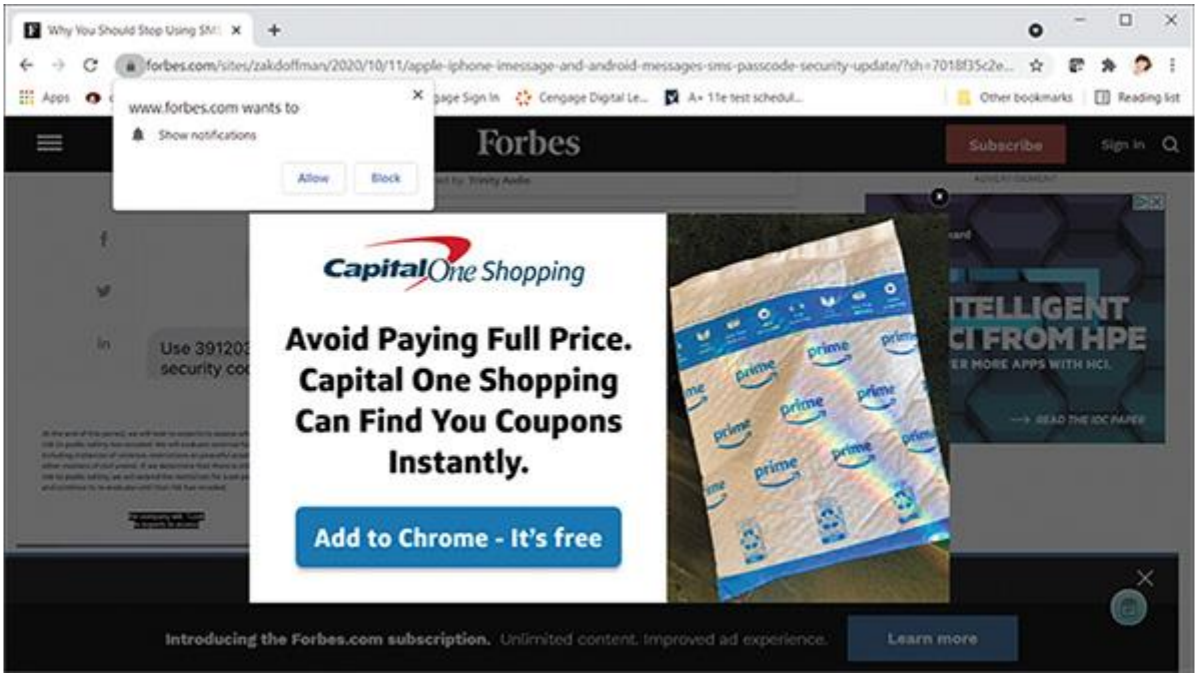
An IT support technician needs to know how to recognize that a system is infected. Here are some warnings that suggest malicious software is at work:

- **Pop-up ads, browser redirection, and desktop alerts.** Basically, a user is losing control of their system. Pop-up ads (see Figure 16-20) are randomly appearing and the browser home page has changed. A browser might also have an uninvited toolbar. The user enters the URL for one website and another site appears in the browser window.

Security alerts—real or spoofed—regularly appear on the desktop to interrupt the user's activity.

Figure 16-20

Random and frequent pop-up ads indicate malware


Why You Should Stop Using SMS
forbes.com/sites/zakdoffman/2020/10/11/apple-iphone-imessage-and-android-messages-sms-passcode-security-update/?sh=7018f35c2e...
Apps
Other bookmarks
Reading list
www.forbes.com wants to
Show notifications
Allow
Block
Forbes
Subscribe
Sign in
Capital One Shopping
Avoid Paying Full Price. Capital One Shopping Can Find You Coupons Instantly.
Add to Chrome - It's free
prime
ITELLIGENT
CI FROM HPE
Use 391203
security co
Introducing the Forbes.com subscription. Unlimited content. Improved ad experience.
Learn more

Source: Forbes

- **Unable to access the network or the Internet, application crashes, and OS update failures.** These types of problems seem to plague the system with no reasonable explanation that is specific to the network, application, or Windows update.
- **Rogue antivirus software and false alerts.** You see false alerts from software that claims to be antivirus software protecting your system. When the user tries to run Microsoft Defender Antivirus (anti-malware software embedded in Windows 10/11), it refuses to run. In the Windows Security window, you find that Defender Antivirus has been disabled because other antivirus software the user did not install is running.

Note 5

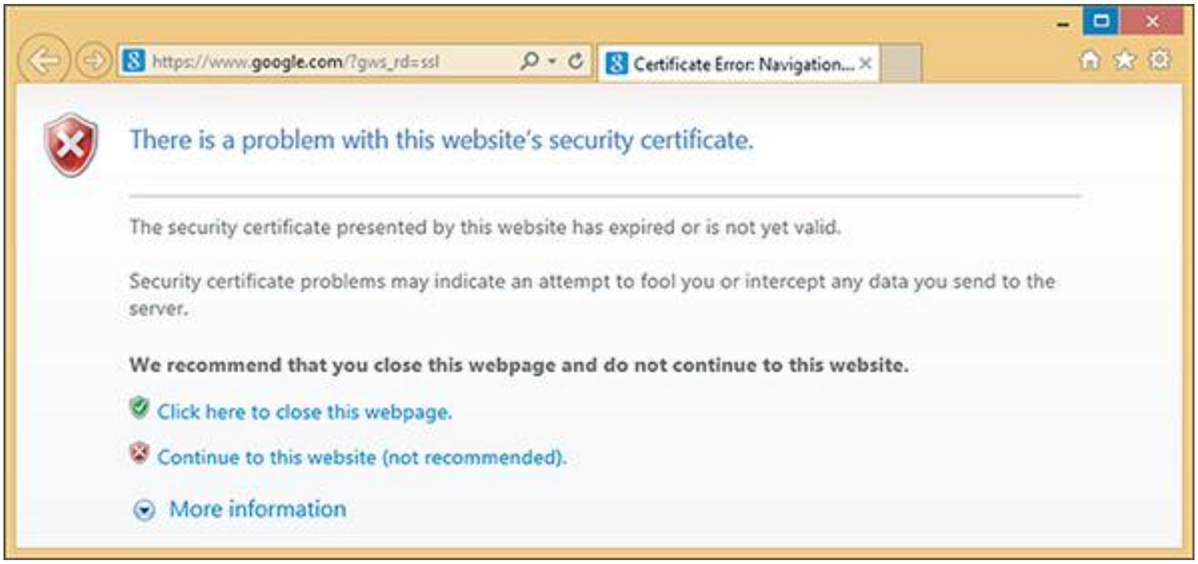
Windows allows only one anti-malware product to run at a time. You can use Task Manager to stop the rogue antivirus software and then start Microsoft Defender Antivirus.

- **Strange notifications and slow performance.** Generally, the system works much slower than before. Programs take longer than normal to load. Strange or bizarre error messages appear. Programs that once worked now give errors. Task Manager shows unfamiliar processes running. The computer's operating system might lock up.

- **Problems with files.** Personal files now have weird names or their file sizes seem excessively large. Executable files have changed size or file extensions change without reason. Files mysteriously disappear or appear. Windows system files are renamed. Files constantly become corrupted. Files you could once access now give access-denied messages, and file permissions change.
- **Problems updating your anti-malware software.** Even though you can browse to other websites, you cannot access anti-malware software sites such as symantec.com or mcafee.com, and you cannot update your anti-malware software.
- **Certificate warnings.** An OS is responsible for validating certificates used to secure communication. For Windows, Microsoft maintains a database of trusted root certificates issued by Certificate Authorities (CAs). A **root certificate** is the original certificate issued by the CA. When a Windows system opens a secure email or visits a secure website and encounters a new digital certificate, it requests Microsoft's trusted root certificate, which is downloaded to the computer. The download happens seamlessly without the user's knowledge unless there's a problem. If Windows cannot obtain the root certificate to validate the email or website, it displays an error (see Figure 16-21). Don't trust websites or email whose certificates have expired or have been revoked.

Figure 16-21

Windows reports a problem with a digital certificate


https://www.google.com/?gws_rd=ssl
Certificate Error: Navigation...

There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

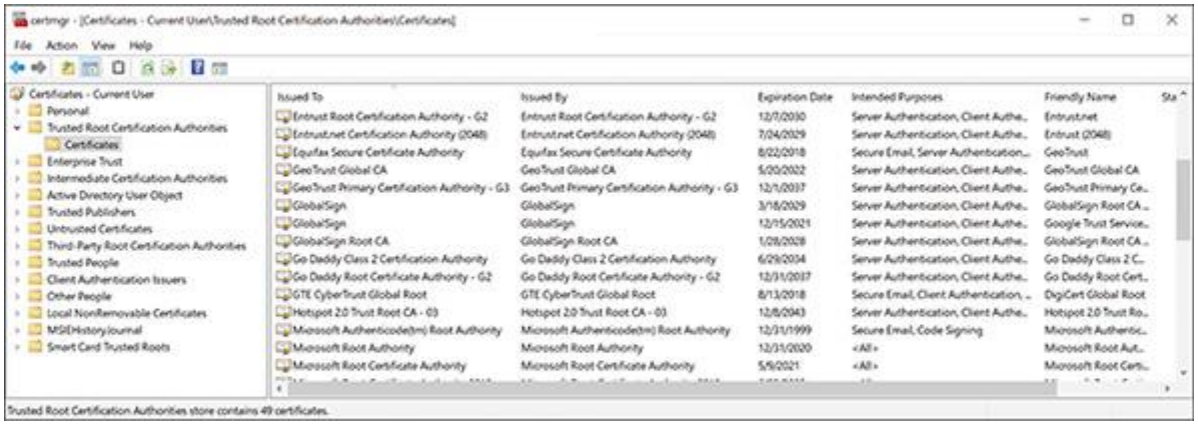
Note 6

If a computer gives certificate warnings, check that the Windows date is correct. A wrong Windows date before the certificate was issued can cause the problem.

You can use the **Certificate Manager** (certmgr.msc) in the Microsoft Management Console (MMC) to view and delete root certificates, as shown in Figure 16-22. For example, the Superfish virus injects a rogue root certificate into the Microsoft store of trusted certificates on the local computer so it can perform an in-path attack to display adware on secure websites a user visits. If you see a Superfish certificate listed among trusted root certificates, be sure to delete it.

Figure 16-22

Windows Certificate Manager can be used to view and delete root certificates kept in the store of trusted certificates



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Other People
Local NonRemovable Certificates
MSIEHistoryJournal
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Sta
Entrust Root Certification Authority - G2	Entrust Root Certification Authority - G2	12/7/2030	Server Authentication, Client Authe...	Entrust.net	
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority (2048)	7/24/2029	Server Authentication, Client Authe...	Entrust (2048)	
Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Server Authentication...	GeoTrust	
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Server Authentication, Client Authe...	GeoTrust Global CA	
GeoTrust Primary Certification Authority - G3	GeoTrust Primary Certification Authority - G3	12/1/2037	Server Authentication, Client Authe...	GeoTrust Primary Ce...	
GlobalSign	GlobalSign	3/18/2029	Server Authentication, Client Authe...	GlobalSign Root CA ...	
GlobalSign	GlobalSign	12/15/2021	Server Authentication, Client Authe...	Google Trust Service...	
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authentication, Client Authe...	GlobalSign Root CA ...	
Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Authority	6/29/2034	Server Authentication, Client Authe...	Go Daddy Class 2 C...	
Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	12/31/2037	Server Authentication, Client Authe...	Go Daddy Root Cert...	
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client Authentication, ...	DigiCert Global Root	
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Server Authentication, Client Authe...	Hotspot 2.0 Trust Ro...	
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	12/31/1999	Secure Email, Code Signing	Microsoft Authentic...	
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...	
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Certi...	

Trusted Root Certification Authorities store contains 49 certificates.

✔ Exam Tip

The A+ Core 2 exam might give you a scenario that requires you to recognize the common symptoms of malware listed previously and to know how to quarantine and remediate an infected system.

16-2eStep 2: Quarantining an Infected System

Core 2 Objective

- 3.3

Given a scenario, use best practice procedures for malware removal.

If an infected computer is connected to a wired or wireless network, immediately disconnect the network cable or turn off the wireless adapter. You don’t want to spread a virus or worm to other computers on your network. A **quarantined computer** is not allowed to use the regular network that other computers use. If you need to use the Internet to download anti-malware software or its updates, take some precautions first. Consider your options. Can you disconnect other computers from the network while the infected computer is connected? Can you isolate the computer from your local network and connect it directly to the ISP or a special quarantined network? If neither option is possible, try downloading the anti-malware software updates while the computer is booted into Safe Mode with Networking or after a clean boot. (Safe Mode doesn't always allow downloads.) Malware might still be running in Safe Mode or after a clean boot, but it's less likely to do so than when the system is started normally.

Always keep in mind that data on the hard drive might not be backed up. Before you begin cleaning up the system, back up data to another media.

16-2fStep 3: Disabling System Protection

Core 2 Objective

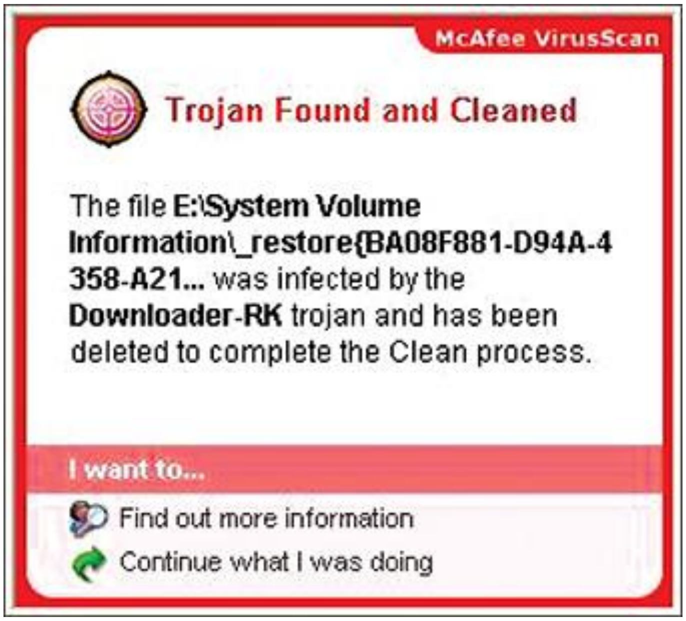
- 3.3

Given a scenario, use best practice procedures for malware removal.

In Windows, some malware hides its program files in restore points stored in the System Volume Information folder that's maintained by System Protection. If System Protection is on, anti-malware software can't clean this protected folder. To get rid of the malware, turn off System Protection so anti-malware software can clean the System Volume Information folder (see Figure 16-23). Realize that when you turn off System Protection, all your restore points are lost, so first consider whether you might need those restore points to troubleshoot the malware infection before you disable System Protection. Also consider that a restore point might be infected and, when applied, might reintroduce the malware back into the system.

Figure 16-23

Malware found in a restore point



McAfee VirusScan

Trojan Found and Cleaned

The file **E:\System Volume Information_restore{BA08F881-D94A-4358-A21...** was infected by the **Downloader-RK** trojan and has been deleted to complete the Clean process.

Source: McAfee Inc.

To turn off System Protection, right-click **Start**, click **System**, and in the About window, click **System protection**. Later, when you are sure the system is clean, turn System Protection back on, and create a new restore point that you can use in the future if problems arise.

Caution

Some highly infected systems will not allow anti-malware software to run. In this situation, you can boot the computer into Safe Mode and use System Restore to apply a restore point that was taken before the infection. Applying a restore point cannot be counted on to completely remove an infection, but it might remove startup entries the malware is using, making it possible to run the anti-malware software from the normal Windows desktop or to run the software in Safe Mode. Consider that you might need to apply a restore point before you disable System Protection, which deletes all your restore points.

16-2gStep 4: Remediating the Infected System

Core 2 Objectives

- 2.5

  Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
- 3.3

  Given a scenario, use best practice procedures for malware removal.

Microsoft Defender Antivirus software is embedded in Windows 10/11 and activated by default. Table 16-1 lists other popular anti-malware software for personal computers and their websites, which also provide information about malware. Before selecting a product, be sure to read some reviews about it and check out some reliable websites that rate anti-malware software. Don’t make the mistake of using an infected computer to purchase and download anti-malware software because keyloggers might be spying and collecting credit card information.

Table 16-1

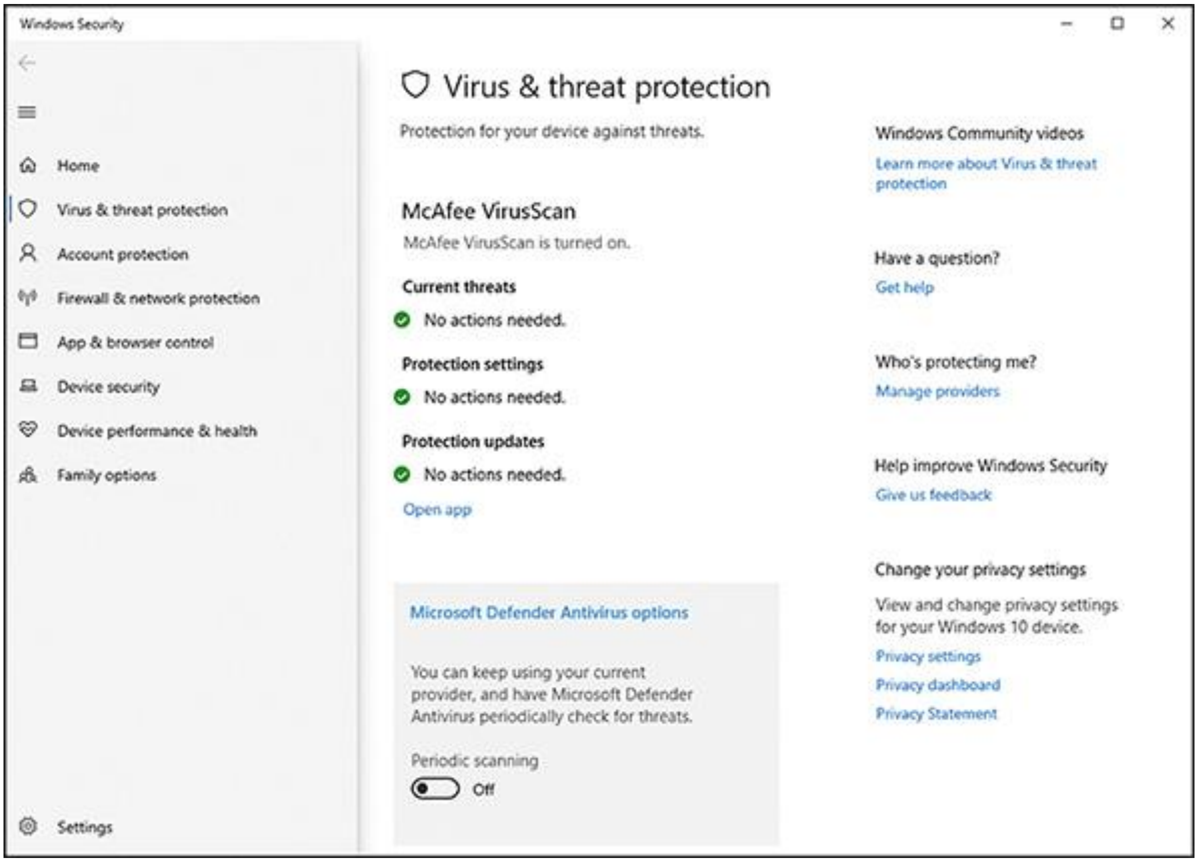
Anti-Malware Software and Websites

Anti-Malware Software	Website
Malwarebytes Premium	malwarebytes.com
Norton AntiVirus Plus	norton.com
Bitdefender Antivirus Plus	bitdefender.com
Kaspersky Anti-Virus	kaspersky.com
McAfee AntiVirus Plus	mcafee.com

To find out what anti-malware software is installed and turned on, in the Windows 10 Settings app, open **Update & Security**, click **Windows Security**, and then click **Virus & threat protection** (see Figure 16-24). If third-party software is running, Defender Antivirus is deactivated by default. For Windows 11, in the Settings app, click **Privacy & security**, **Windows Security**, and **Virus & threat protection**.

Figure 16-24

McAfee VirusScan is protecting the system rather than Microsoft Defender Antivirus, the default Windows solution



Virus & threat protection

Protection for your device against threats.

McAfee VirusScan

McAfee VirusScan is turned on.

Current threats

No actions needed.

Protection settings

No actions needed.

Protection updates

No actions needed.

Open app

Microsoft Defender Antivirus options

You can keep using your current provider, and have Microsoft Defender Antivirus periodically check for threats.

Periodic scanning

Off

Windows Community videos

Learn more about Virus & threat protection

Have a question?

Get help

Who's protecting me?

Manage providers

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

Privacy Statement

Caution

Beware of websites that appear as sponsored links at the top of search results for anti-malware software. These sites might appear to be the home site for the software, but they are really trying to lure you into downloading adware or spyware.

Now let’s look at different situations you might encounter when attempting to run anti-malware software.

Update and Run Anti-Malware Software

Anti-malware software can’t find what it doesn’t know to look for. As new malware gets into the wild (becomes available on the Internet), anti-malware software needs to be updated with these latest **malware definitions**, also called **malware signatures**. Do the following to update and run the software:

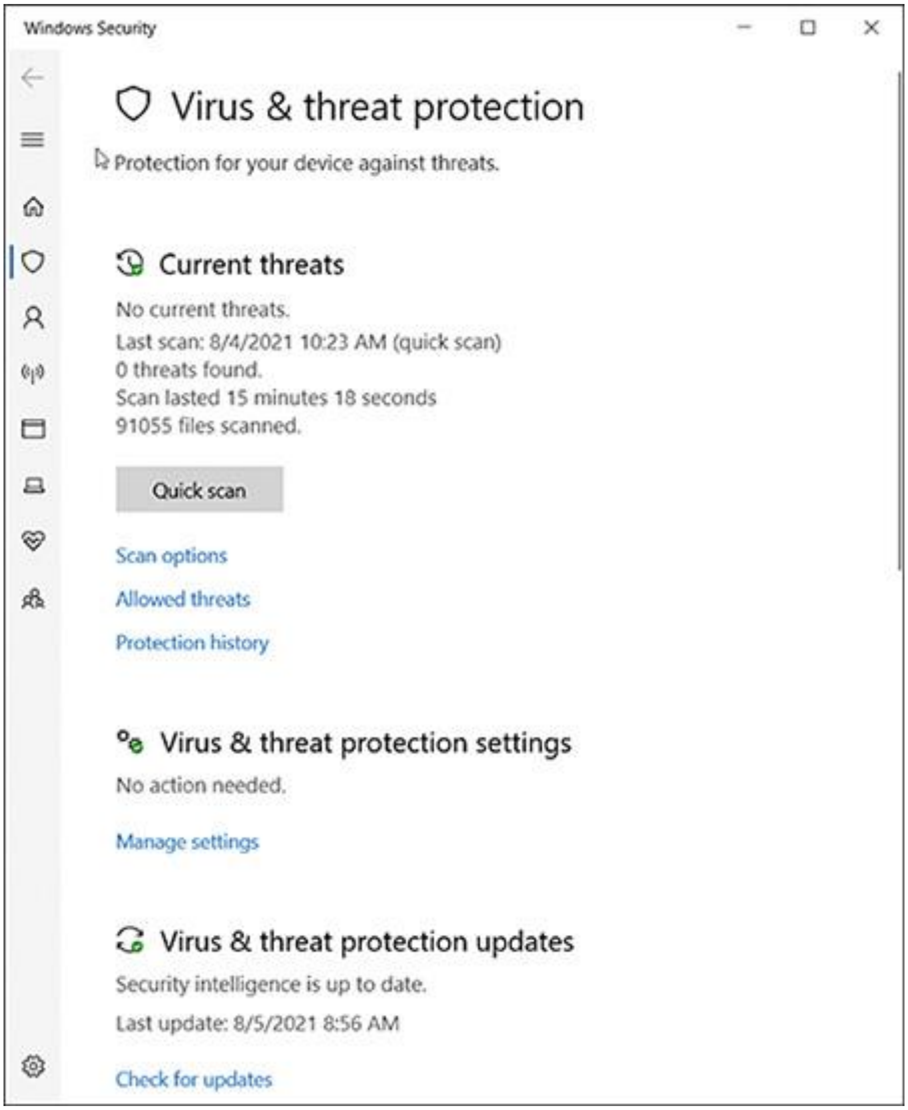
- 1.

  Verify the anti-malware software is up to date. Microsoft Defender Antivirus normally gets its updates in Windows security updates. To manually check for updates for Windows 10 Defender Antivirus, in Settings, open **Update & Security**, click **Windows Security**, and click **Virus & threat protection**. In the Virus & threat protection window (see Figure 16-25), click **Check for updates**. For Windows

11, in Settings, click **Privacy & security, Windows Security**, **Virus & threat protection**, **Protection updates**, and **Check for updates**. If you are using third-party anti-malware, open the app and look for the update feature in the app’s window.

Figure 16-25

Manually update Microsoft Defender Antivirus



Windows Security

Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 8/4/2021 10:23 AM (quick scan)
0 threats found.
Scan lasted 15 minutes 18 seconds
91055 files scanned.

Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

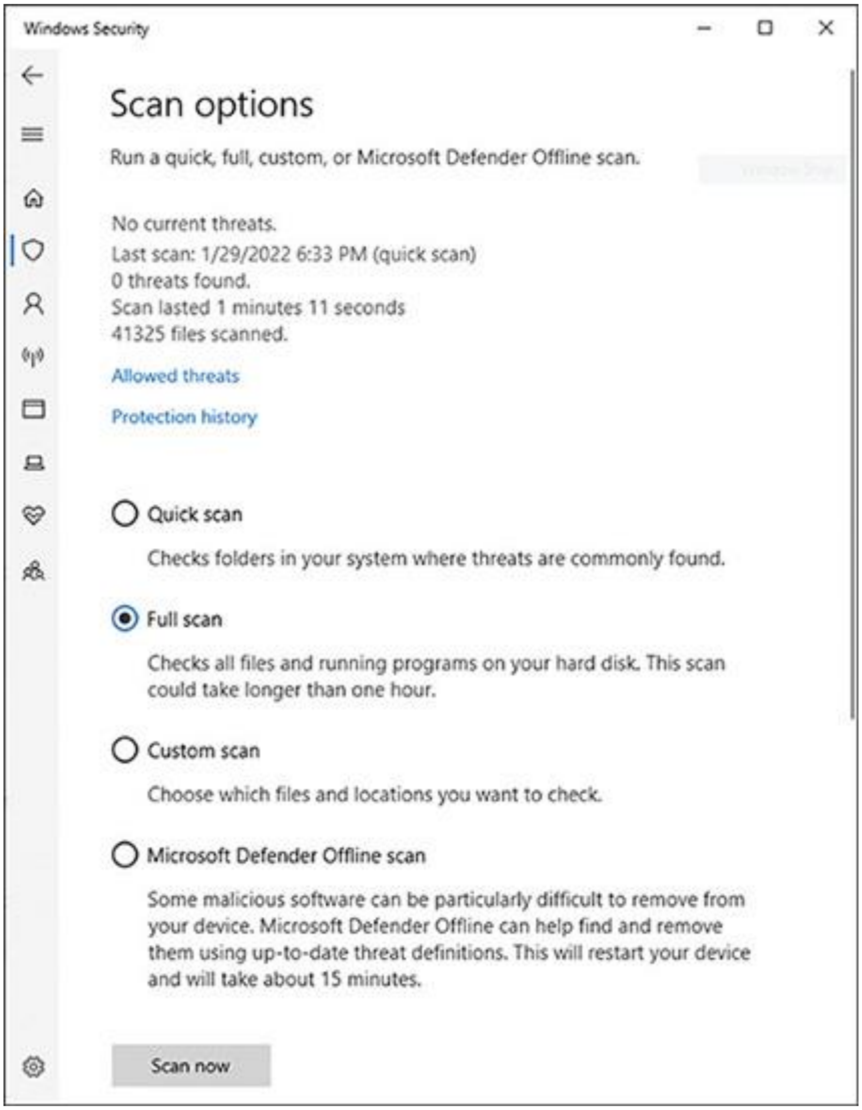
Last update: 8/5/2021 8:56 AM

- 2.

  Use the anti-malware software to perform a full scan of the system. For example, for Defender Antivirus, in the *Virus & threat protection* window (see Figure 16-25), click **Scan options**. In the Scan options window (see Figure 16-26), select **Full scan** and click **Scan now.** As it scans, the software might ask you what to do with an infected program (see Figure 16-27), or it might log the event in an event viewer or history log it keeps. In most situations, you would delete an infected program.

Figure 16-26

A full scan can take some time and is preferred when a virus is suspected



Windows Security

Scan options

Run a quick, full, custom, or Microsoft Defender Offline scan.

No current threats.
Last scan: 1/29/2022 6:33 PM (quick scan)
0 threats found.
Scan lasted 1 minutes 11 seconds
41325 files scanned.

Allowed threats

Protection history

○ Quick scan

Checks folders in your system where threats are commonly found.

● Full scan

Checks all files and running programs on your hard disk. This scan could take longer than one hour.

○ Custom scan

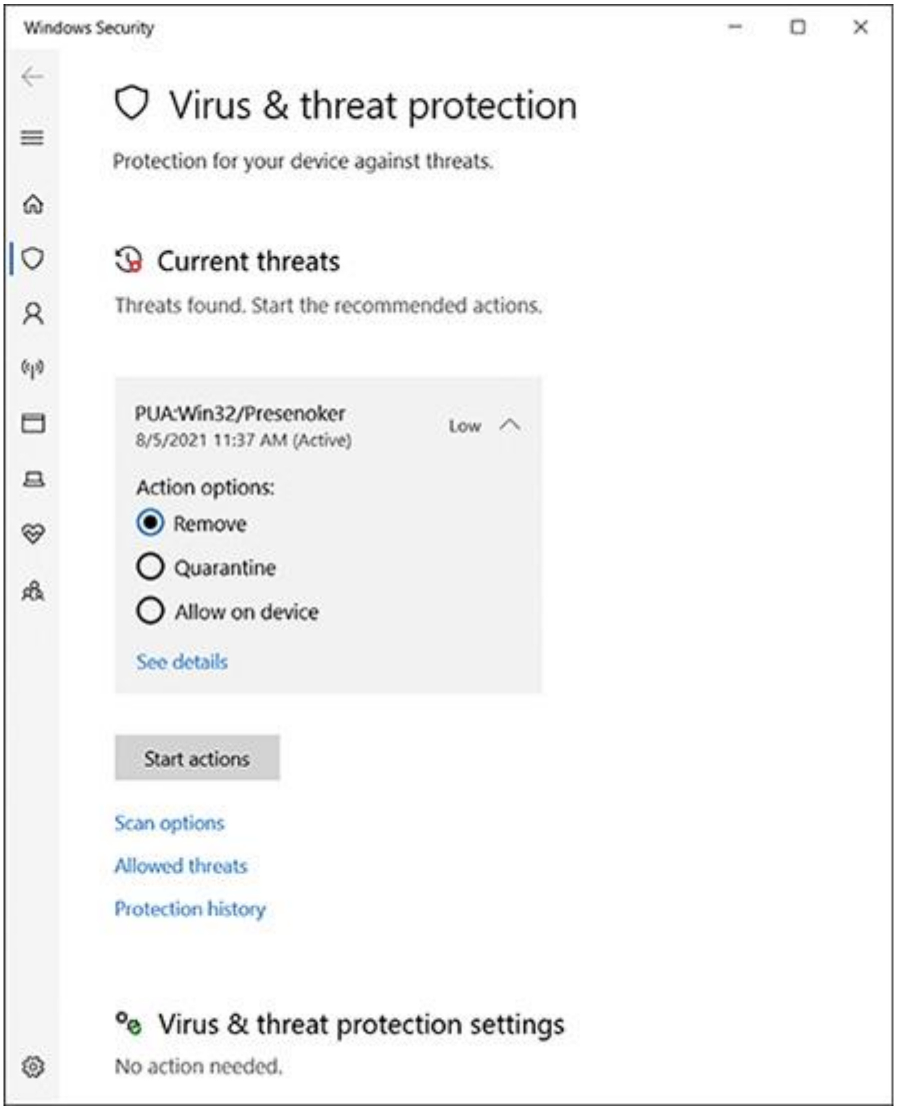
Choose which files and locations you want to check.

○ Microsoft Defender Offline scan

Some malicious software can be particularly difficult to remove from your device. Microsoft Defender Offline can help find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

Figure 16-27

It is better to remove a threat rather than quarantine or allow it



Virus & threat protection

Protection for your device against threats.

Current threats

Threats found. Start the recommended actions.

PUA:Win32/Presenoker
8/5/2021 11:37 AM (Active)   Low

Action options:

● Remove

○ Quarantine

○ Allow on device

Virus & threat protection settings

No action needed.

- 3.

  After the scan is complete and you have decided what to do with each suspicious file, reboot the system, allow the software to update itself again, and then scan the system again. Most likely, some new malware will be discovered. Keep rebooting and rescanning until a scan comes up clean.

Note 7

If you ever encounter a virus that your updated anti-malware software did not find, be sure to let the manufacturer of the software know so they can research the problem.

When Anti-Malware Software Gives Errors

If Defender Antivirus detects malware it cannot remove, it asks permission to run Microsoft Defender Offline. When you agree, the system reboots and runs a scan in the recovery environment (preinstallation environment). Defender Offline can detect and remove rootkits, boot sector viruses, and other persistent malware that cannot be dealt with after Windows starts. If Defender Antivirus or third-party anti-malware software refuses to run or runs with errors, follow these steps:

1. 1

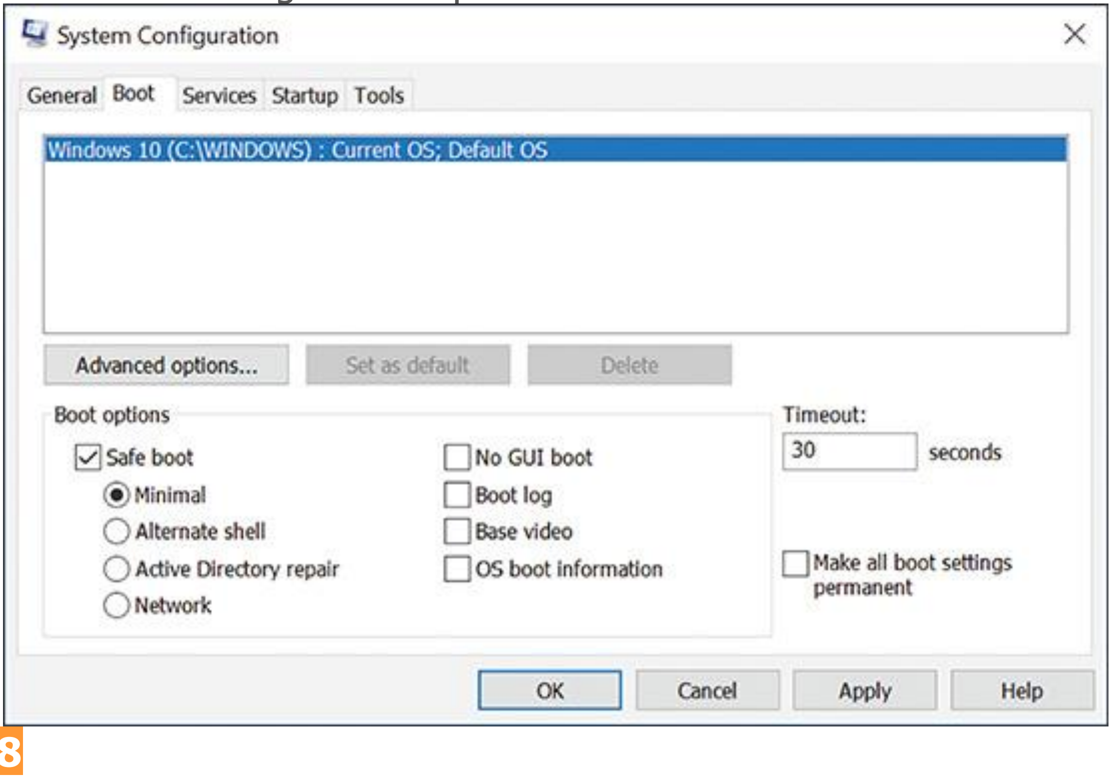
   Perform a Microsoft Defender Offline scan. Sign in to Windows using an administrator account. In the Scan options window (refer back to Figure 16-26), select **Microsoft Defender Offline scan**, and click **Scan now**. Respond to the UAC dialog box. The computer reboots in the preinstallation environment and scans the system.

2. 2

   Boot into Safe Mode and scan the system. Some malware prevents anti-malware software from running. In this situation, try booting the system in Safe Mode or performing a clean boot and then running the anti-malware software. Recall that to launch Windows in Safe Mode, also called Safe boot, enter the `msconfig` command in the Windows search box. In the System Configuration dialog box, click the **Boot** tab and check **Safe boot** (see Figure 16-28). To launch Safe Mode with Networking so you can update your anti-malware software, select **Network** in the list of options. Then restart the system.

Figure 16-28

Use the Safe boot option to boot the system in Safe Mode and prevent malware from launching at startup



Windows 10 (C:\WINDOWS) : Current OS; Default OS

Boot options

☑ Safe boot

● Minimal

○ Alternate shell

○ Active Directory repair

○ Network

□ No GUI boot

□ Boot log

□ Base video

□ OS boot information

Timeout: 30 seconds

□ Make all boot settings permanent

Note 8

If viruses are launched even after you boot in Safe Mode and you cannot get the anti-malware software to work, try searching for suspicious entries in the Windows registry subkeys under HKLM\System\CurrentControlSet\Control\SafeBoot. Subkeys under this key control what is launched when you boot into Safe Mode. How to edit the registry is covered in the module “Troubleshooting Windows After Startup.”

3. 3

   Scan the system using a healthy networked computer. Follow these steps:

   1. a

      On the infected computer, share drive C: so you can reach it from another computer.

   2. b

      Make sure the remote computer has its software firewall set for maximum protection and its installed anti-malware software is up to date and running.

   3. c

      Network the two computers. (Don’t connect the infected computer to the entire network. If necessary, you can connect the two computers using a crossover cable or using a small switch and network cables.)

   4. d

      To make your work easier, you can map a network drive from the remote computer to drive C: on the infected computer.

   5. e

      Perform an anti-malware scan on the remote computer, pointing the scan to drive C: on the infected computer. For Defender Antivirus, open the **Scan options** window (refer back to Figure 16-26), select **Custom scan**, click **Scan now**, and point to the infected computer under Network.

Note 9

How to network two computers with a switch and cables is covered in the Core 1 module, “Networking Fundamentals.” How to share a drive or folder and how to mount a network drive are covered in the module, “Securing and Sharing Windows Resources.”

When an Infected Computer Will Not Boot

If an infected computer will not boot, the boot manager, boot loaders, or kernel mode drivers launched at startup might be infected or damaged. Launch the computer into Windows Recovery Environment (Windows RE), and use the Startup Repair process to repair the system. The module “Troubleshooting Windows Startup” gives more information about solving boot problems. You can also install the hard drive as a second drive in another system and use that system to scan the drive for malware.

Note 10

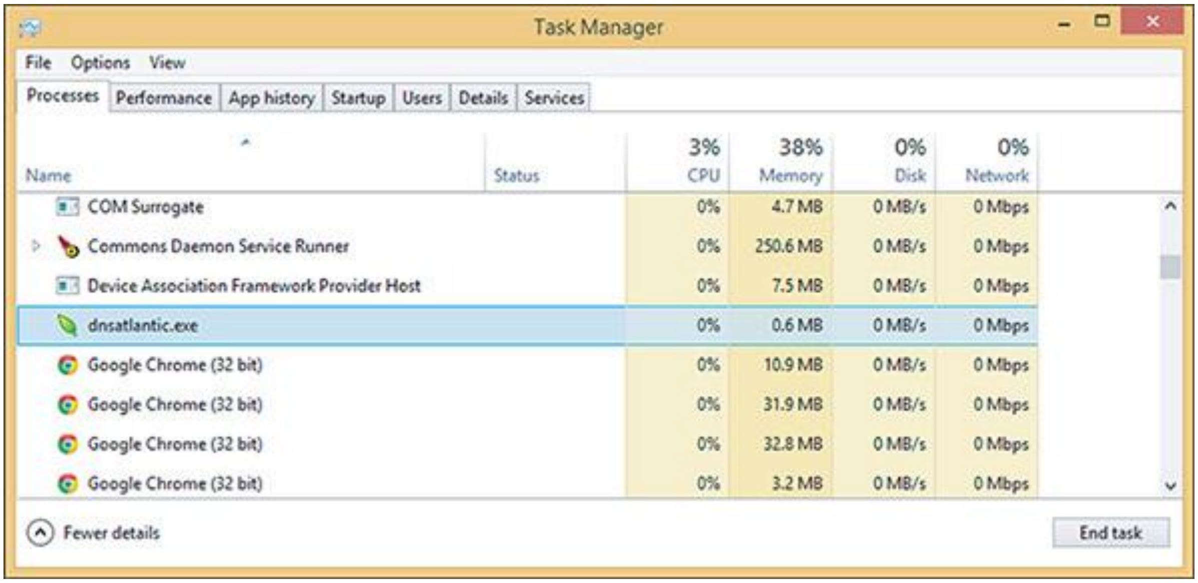
Some anti-malware companies offer preinstallation scanning tools, also called rescue disks or bootable antivirus tools. One example is Kaspersky's Rescue Disk (kaspersky.com), which is free. You learn how to use the disk in a project at the end of this module.

Run More Than One Scan of Anti-Malware Software

After you've scanned the system using one of the methods just discussed, reboot, update the software, and then keep scanning and rebooting until the scan report is clean. If a second or third scan doesn't remove all symptoms of malware, consider installing and running a second anti-malware program. What one anti-malware program cannot detect or remove, another one might. For example, Defender Antivirus on one system removed malware it detected, but did not detect or remove the downloader *dnsatlantic.exe*, which hijacked a browser and is still running in the background (see Figure 16-29).

Figure 16-29

The malware downloader *dnsatlantic.exe* is still running after multiple scans of anti-malware software



Name	Status	3% CPU	38% Memory	0% Disk	0% Network
COM Surrogate		0%	4.7 MB	0 MB/s	0 Mbps
Commons Daemon Service Runner		0%	250.6 MB	0 MB/s	0 Mbps
Device Association Framework Provider Host		0%	7.5 MB	0 MB/s	0 Mbps
dnsatlantic.exe		0%	0.6 MB	0 MB/s	0 Mbps
Google Chrome (32 bit)		0%	10.9 MB	0 MB/s	0 Mbps
Google Chrome (32 bit)		0%	31.9 MB	0 MB/s	0 Mbps
Google Chrome (32 bit)		0%	32.8 MB	0 MB/s	0 Mbps
Google Chrome (32 bit)		0%	3.2 MB	0 MB/s	0 Mbps

In this situation, try another anti-malware program. For example, Microsoft Safety Scanner (docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download) is not designed for ongoing malware prevention but can sometimes remove malware that Defender Antivirus did not find. Download and run the latest version of the software.

Clean Up What’s Left Over

Next, you’ll need to clean up anything the anti-malware software left behind. Sometimes anti-malware software tells you it is not able to delete a file, or it deletes an infected file but leaves behind an orphaned entry in the registry or startup folders. If the anti-malware software tells you it was not able to delete or clean a file, first check the anti-malware software website for any instructions you might find to manually clean things up. Here are some general actions you can take to clean up what the software left behind:

1. **Respond to any startup errors.** On the first boot after anti-malware software has declared a system clean, you might still find some startup errors caused by incomplete removal of the malware. Use Task Manager to find out how a startup program is launched. If the program is launched from the registry, you can back up and delete the registry key. If the program is launched from a startup folder, you can move or delete the shortcut or program in the folder. See the appendix “Entry Points for Windows Startup Processes” for a list of startup folders and startup registry keys.
2. **Research malware types and program files.** Your anti-malware software might alert you to a suspicious program file that it quarantines and then ask you to decide if you want to delete it. The web is your best tool to use when making your decision about a program. Some websites that offer **malware encyclopedias** that are reliable and give you symptoms and solutions for malware include the following:

    - Process Library by ProcessLibrary at processlibrary.com
    - DLL Library by Uniblue Systems Limited at liutilities.com
    - All the anti-malware software sites listed earlier in Table 16-1

    Beware of using other sites! Much information on the web is written by people who are just guessing, and some of the information is put there to purposefully deceive. Check things out carefully, and learn which sites you can rely on.

3. **Delete files.** For each program file the anti-malware software told you it could not delete, delete the program file yourself by following these steps:

    - a

      First try Explorer to locate a file and delete it. For peace of mind, don’t forget to empty the Recycle Bin when you’re done.

    - b

      If the file is hidden or access is denied, open an elevated command prompt window and use the commands listed in Table 16-2 to take control of a file so you can delete it. If the commands don't work using an elevated command prompt window, use the commands in a command prompt window in Windows RE.

Table 16-2

Commands Used to Take Control of a Malware File So You Can Delete It

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>attrib –r –s <i>filename.ext</i></td><td>Remove the read-only and system attributes to a file.</td></tr>
<tr><td>tasklist | more
taskkill /f /pid:<i>9999</i></td><td>To stop a running process, first use the tasklist command to find ou the process. Then use the taskkill command to forcefully kill the pro process ID.</td></tr>
<tr><td>takeown /f <i>filename.ext</i></td><td>Take ownership of a file.</td></tr>
<tr><td>icacls <i>filename.ext</i> /grant administrators:f</td><td>Take full access of a file.</td></tr>
</table>

- c

  To get rid of other malware files, use the Disk Cleanup process in the Drive C: properties dialog box, or delete the browsing history using the Internet Options dialog box.

- d

  Delete all subfolders and files in the C:\Windows\Temp folder, which Trojan downloaders are likely to use.

4. **Clean up your browsers and uninstall unwanted programs.** Adware and spyware might install add-ons to a browser (including toolbars you didn't ask for), install cookie trackers, and change your browser security settings. Anti-malware software might have found all these items, but as a good defense, take a few minutes to find out for yourself. The module "Network Security and Troubleshooting" covers how to use the Internet Options dialog box to search for unwanted add-ons and delete ActiveX controls. You can uninstall unwanted toolbars, plug-ins, and other software using the Programs and Features window.

16-2hStep 5: Protecting the System with Scheduled Scans and Updates

Core 2 Objective

- 3.3

Given a scenario, use best practice procedures for malware removal.

Once your system is clean, you'll certainly want to keep it that way. The following are three best practices to protect a system against malware:

- **Use anti-malware software.** Microsoft Defender Antivirus is enabled and automatically updated by default. If you decide to use other anti-malware software, configure the software so it
  1. runs in the background in real time to alert users of malware that attempts to run or install,
  2. automatically scans incoming email attachments, and
  3. performs scheduled scans of the system and automatically downloads updates to the software.
- **Always use a software firewall.** Never, ever connect your computer to an unprotected network without using a firewall. Windows Defender Firewall is turned on by default. Recall that you can configure Windows Defender Firewall to allow no uninvited communication or to allow the exceptions that you specify. Details about Windows Defender Firewall are covered in the module "Network Security and Troubleshooting."
- **Keep Windows updates current.** Microsoft continually releases updates to plug vulnerable entrances in Windows where malware might attack and updates to Defender Antivirus. Recall that you can verify Windows Update settings in the Settings app.

16-2iStep 6: Enabling System Protection and Creating a Restore Point

Core 2 Objective

- 3.3

Given a scenario, use best practice procedures for malware removal.

Now that the system is clean, you can turn System Protection back on if necessary and create a restore point. You learned how to do this in the module “Maintaining Windows.”

16-2jStep 7: Educating the End User

Core 2 Objectives

- 2.3

  Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.
- 3.3

  Given a scenario, use best practice procedures for malware removal.

Now would be a good time to sit down with the user and go over the tips presented earlier in this module to keep the system free from malware. Sometimes the most overlooked step in preventing malware infections is to educate the user. Even with all your security measures in place, a user can still download and execute a Trojan, which can install more malware in the system.

✓ Exam Tip

The A+ Core 2 exam might give you a scenario that requires you to perform one or more of the seven steps to remove malware. Memorize these seven steps and know how to use them in the correct order.

Now we turn our attention to other ways an IT technician might be called on to protect data and other resources, including enforcing licensing and security policies and protecting regulated data.

16-3Licensing, Regulated Data, and Security Policies

Core 2 Objectives

- 2.6

  Given a scenario, configure a workstation to meet best practices for security.
- 2.8

Given a scenario, use common data destruction and disposal methods.

- 4.1

  Given a scenario, implement best practices associated with documentation and support systems information management.

- 4.6

  Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

An IT technician is expected to follow company security policies for software licensing and regulated data. You also need to know what to do if you discover that these policies have been violated.

16-3a Software Licensing and Digital Rights

Core 2 Objective

- 4.6

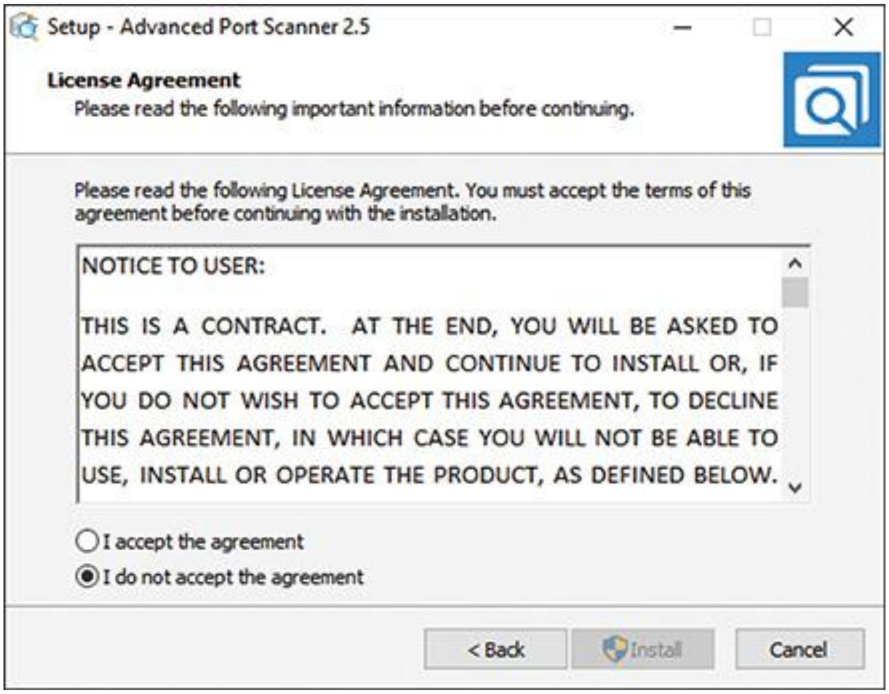
  Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

As an IT support technician, you need to be especially aware of the issues surrounding software licensing. When someone purchases software from a software developer, that person or organization has only purchased a **license** for the software, which is the right to use it. The buyer does not legally own the software and therefore does not have the right to distribute it. Important facts about software licensing include the following:

- **The copyright.** The right to copy the work, called a **copyright**, belongs to the creator of the work or others to whom the creator transfers this right. Copyrights are intended to legally protect the intellectual property rights of organizations or individuals to creative works, which include books, images, and software.
- **The EULA.** Your rights to use or copy software are clearly stated in the **End User License Agreement (EULA)** that you agree to when you install the software (see Figure 16-30). The EULA is a legally binding contract between the user and software owner. If the user violates the agreement, the software license is no longer valid. A non-expiring software license does not require renewing, or the license might be valid only for a period of time.

Figure 16-30

Agreeing to the EULA is required before software installs



Setup - Advanced Port Scanner 2.5

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

NOTICE TO USER:

THIS IS A CONTRACT. AT THE END, YOU WILL BE ASKED TO ACCEPT THIS AGREEMENT AND CONTINUE TO INSTALL OR, IF YOU DO NOT WISH TO ACCEPT THIS AGREEMENT, TO DECLINE THIS AGREEMENT, IN WHICH CASE YOU WILL NOT BE ABLE TO USE, INSTALL OR OPERATE THE PRODUCT, AS DEFINED BELOW.

○ I accept the agreement

● I do not accept the agreement

Source: Famatech Corp.

- **Software piracy.** Making unauthorized copies of original software violates the Federal Copyright Act of 1976 and is called **software piracy** or, more officially, software copyright infringement. (This act allows for one backup copy of software to be made.) Making a copy of software and then selling it or giving it away is a violation of the law. Normally, only the employee who violates the copyright law is liable for infringement; however, in some cases, an employer or supervisor is also held responsible, even when the copies were made without the employer's knowledge.

Note 11

When an individual or organization purchases the right to install one instance of software, the license is called a **personal use license**. By purchasing a **site license**, also called a **commercial use license**, a company can obtain the right to multiple installations of software.

- **Digital rights management.** Many software companies, including Microsoft, have implemented measures to control the use of their software, a practice called **digital rights management (DRM)**. For example, recall that the retail release of Windows 10/11 requires a valid product key or a digital license for activation, and Microsoft carefully verifies and monitors that this product key is used only in one installation.
- **Open-source license.** As you have learned, **open-source software** (such as Linux OS and Apache web server) is developed in a public, collaborative way and can be used for any purpose. **Closed-source software** (such as Windows or PhotoShop) is owned by the

creator (developer). When you download open-source software, you must agree to a EULA that describes how you can use the software and receive an **open-source license**. Two popular types of open-source licenses are

- **Copyleft.** A copyleft open-source license allows you to use the software for free, but you cannot sell it or sell modified versions of it to others.
- **Permissive.** With a permissive open-source license, anything goes. You can use it for free, modify it, and sell it.

16-3bRegulated Data and Compliance Policies

Core 2 Objectives

- 2.6

  Given a scenario, configure a workstation to meet best practices for security.
- 4.6

  Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

Certain types of data are protected by special governmental regulations and are called **regulated data**; this data must be provided to the regulatory agency on demand. In addition, each industry must comply with a variety of regulations, policies, and laws, which are collectively called **regulatory and compliance policies**. For example, in the healthcare industry, patient data is highly regulated, and most hospitals employ one or more regulatory and compliance officers to ensure that the hospital is compliant. Other areas of regulation include copyright laws regulated by the U.S. Copyright Office, workplace safety regulated by the Occupational Safety and Health Administration (OSHA), and consumer protection regulated by the Federal Trade Commission (FTC). Many of these policies directly affect IT operations. When you're first hired by a company, you should receive training on how these issues affect your work and what is expected of you.

Note 12

An IT technician needs to know their organization's **data retention** policy for regulated data, which can include the number of years regulated data must be retained after a termination date.

Let's look at some specific types of regulated data:

- **Personal identity.** **PII (personally identifiable information)** is a legal term to describe data that can uniquely identify a person, including a Social Security number, email address, physical address, birthdate, birthplace, mother's maiden name, marital status, phone numbers, race, and biometric data. Some PII is more sensitive than other information and should be protected more vigilantly.
- **Healthcare data.** **PHI (protected health information)** includes any data about a person's health status or health care. This data is protected by regulations defined by HIPAA (the Health Insurance Portability and Accountability Act), passed in 1996. HIPAA gives patients the rights to monitor and restrict the sharing of their medical information. Hospitals, medical personnel, and other entities covered by HIPAA regulations risk steep penalties for privacy breaches.
- **Credit card data.** The **Payment Card Industry (PCI)** standards were defined to help prevent credit card fraud and are backed by all the major credit card brands (Visa, MasterCard, and others). PCI standards apply to how credit card data is protected in transit (such as when receiving payments) and at rest (when stored, such as when keeping records for recurring billing) by vendors, retailers, and financial institutions.
- **Personal government-issued information.** Documents—including a birth certificate, Social Security card, state-issued driver's license, military ID card, or passport—and biometric data—such as fingerprints—that a government creates or collects to identify a person is regulated in how it can be collected, stored, and shared and how individuals must be noticed if their data is hacked. You also need to know that the GDPR (General Data Protection Regulation) is a group of regulations implemented in 2018 in the European Union (EU) to protect personal data of EU citizens.

Note 13

Organizations and individuals who have access to regulated data are at risk legally and financially if they do not comply with the legal requirements regarding the security of this data. When you work in an organization that handles regulated data, ensure your own protection by making certain you understand and comply with all laws regarding this data.

16-3cData Destruction and Disposal

Core 2 Objective

- 2.8

  Given a scenario, use common data destruction and disposal methods.

As an IT technician, you might be asked to properly dispose of storage media. In addition to the risks posed by dumpster diving, consider its potential impact. Before you throw out a hard drive, flash drive, CD, DVD, tape, or other media that might have regulated or corporate data on it, completely destroy the data on the device. Trying to wipe a drive clean by deleting files or even formatting the drive does not completely destroy the data. Here are some ways to destroy printed documents and sanitize storage devices:

- **Overwrite data on the drive.** A drive needs to be wiped clean before you recycle or repurpose it. Today's devices receive a **low-level format** at the factory, which writes sector marks on a drive. (This is different from a **standard format** in Windows that configures a file system on the drive.) Today's hard drives cannot be low-level formatted by users. However, users can erase or wipe clean a drive using a **zero-fill utility** that overwrites all data on the drive with zeroes; sometimes this is inaccurately called a low-level format. You can download a zero-fill utility or so-called low-level format utility from many hard drive manufacturers' websites. This method works for most low-security situations, but professional thieves know how to break through it. If you use one of these utilities, run it multiple times to write zeroes on top of zeroes. Data recovery has been known to reach 14 levels of overwrites because each bit is slightly offset from the one under it.

Note 14

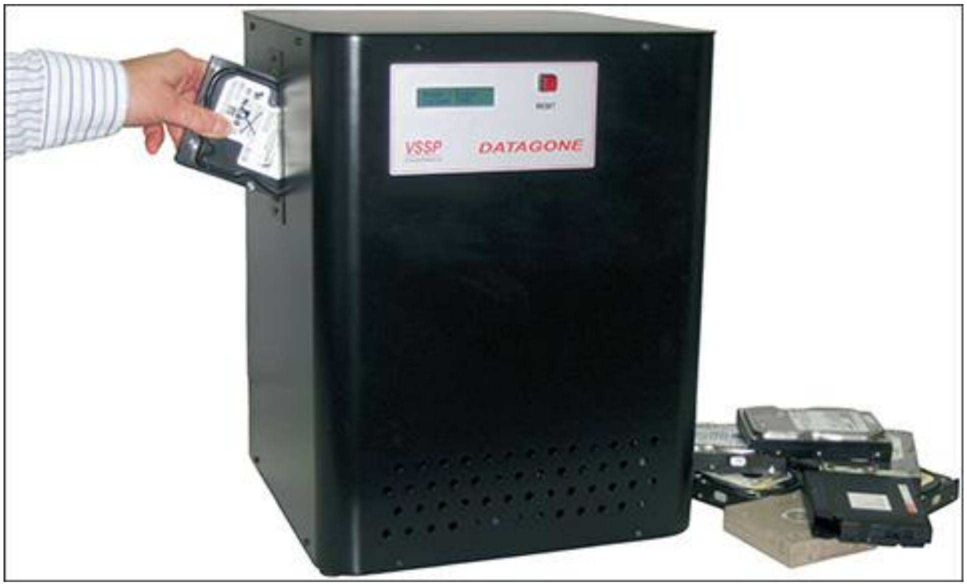
An app called a file shredder can permanently delete an individual file or folder by overwriting it multiple times. Check the reviews before downloading and using one of these apps.

- **For solid-state devices, use a Secure Erase utility.** As required by government regulations for personal data privacy, the American National Standards Institute (ANSI) developed the **ATA Secure Erase** standards to wipe clean a solid-state device such as a USB flash drive or SSD. You can download a Secure Erase utility from the manufacturer of the device and run it to sanitize the drive, or you can securely erase all data on the device and then reuse or dispose of it.
- **Physically destroy the storage media.** Use a drill to drill many holes all the way through the drive housing. Break CDs and DVDs in half, and do similar physical damage with a hammer to flash drives or tapes, even to the point of setting them on fire to incinerate them. Again, expert thieves can still recover some of the data.
- **For magnetic devices, use a degausser.** A **degausser** exposes a storage device to a strong electromagnetic field to completely erase the data on a magnetic hard drive or tape drive (see Figure 16-31). A degaussed drive can't be recycled, but for the best destruction, use the

degausser and physically destroy the drive. Degaussing does not erase data on a solid-state hard drive or other flash media because these devices don't use magnetic surfaces to hold data.

Figure 16-31

Use a degausser to sanitize a magnetic hard drive or tape drive



- **Use a shredder.** You can use a paper **shredder** to destroy all documents that contain sensitive data. The best paper shredders apply multiple passes to crosscut the paper instead of strip-cutting; this cuts the paper into smaller pieces that can't be easily reassembled. Many paper shredders can handle credit cards or thin cardboard. **Multimedia shredders** can also destroy optical discs. **Disk drive shredders**, such as the one from Whitaker Brothers (whitakerbrothers.com) shown in Figure 16-32, can destroy magnetic hard drives, solid-state drives, flash drives, optical discs, and even mobile devices such as smartphones or small tablets.

Figure 16-32

This drive shredder pulverizes small storage devices such as hard drives, flash drives, and smartphones

Source: Whitaker Brothers

- **Use a secure third-party data-destruction vendor.** For the very best data destruction, consider a secure data-destruction service. To find a vendor providing the service, search the web for “secure data destruction.” However, don’t use a service unless you have thoroughly checked its references and guarantees of legal compliance that your organization is required to meet. The service should provide you with a digital **certificate of destruction**, which verifies that the data has been destroyed beyond recovery. Paper certificates can be forged, but digital certificates produced by the software that performs the destruction will provide auditable results of the destruction process.

✔ Exam Tip

The A+ Core 2 exam might give you a scenario that requires you to implement data-destruction techniques, including using a shredder, degausser, incineration, drill, hammer, and recycling or repurposing techniques (low-level formats, overwriting, and drive wipes).

16-3dIncident Response for Prohibited Content and Activities

Core 2 Objectives

- 4.1

  Given a scenario, implement best practices associated with documentation and support systems information management.
- 4.6

  Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

As you know, employees in an organization are often asked to agree to an acceptable use policy (AUP) that documents a code of conduct when using corporate resources. For example, the AUP may prohibit an employee from accessing pornographic material on company computers, using company computers and time for personal shopping, or installing pirated software on these computers.

An **incident** is when an employee or other person has negatively affected safety or corporate resources, violated the code of conduct for the organization, or committed a crime. When you start a new job, ask your employer what procedures you follow for an **incident response**. If you're the first person to discover an incident, such as the intentional misuse of regulated data or other activities, you're responsible to perform certain **first response** duties. One of these tasks is to document what happened in an **incident report**. This report is important to prevent future incidents and crucial to a criminal investigation. Here are some things you need to know:

- **Identify and go through proper channels.** When you identify what you believe to be an infringement of the law or the company's code of conduct, where do you turn to report the issue? To management and/or to law enforcement? Make sure you go only through proper channels; don't spread rumors or accusations.
- **Preserve data and devices.** What data or device should you immediately preserve as evidence for what you believe has happened? For example, if you believe you have witnessed a customer or employee using a company computer for a crime, should you remove and secure the hard drive from the computer, or should you remove and secure the entire computer? Are you expected to make a copy of the data or image the hard drive before you turn the device over to others?

- **Incident documentation. Incident documentation**, also called an **incident report**, surrounding the evidence of an incident is important to prevent future incidents and crucial to a criminal investigation. What documentation are you expected to submit and to whom is it submitted? This documentation might track the **chain of custody (CoC)** for the evidence, which includes exactly what, when, and from whom it was collected, the condition of this evidence, and how the evidence was secured while it was in your possession. Each device or item includes a paper trail of each person to whom the evidence has been passed on and when. For example, suppose you suspect that a criminal act has happened and you hold a flash drive that you believe contains evidence of this crime. You need to carefully document exactly when and how you received the flash drive. Also, don't pass it on to someone else in your organization unless you have the person's signature on a chain-of-custody document so you can later prove you handled the evidence appropriately. You don't want the evidence to be disallowed in a court of law because you have been accused of misconduct or tampering with the evidence. Also know that more information than a signature, such as a copy of a driver's license, might be required to identify people in the chain of custody.

✓ Exam Tip

The A+ Core 2 exam expects you to be able to explain the process of an incident response, which includes reporting prohibited content or activity through the proper channels and to law enforcement as necessary, copying and preserving relevant data and evidence, and tracking evidence through an appropriate chain-of-custody document.

Module Review

16-4a Module Summary

Physical and Logical Security

- Physical security can include security fences, bollards, access control vestibules, guards, video surveillance, alarm systems, magnetometers (metal detectors), locks and keys, port locks, privacy screens, and theft-prevention plates.
- Staff access to resources is controlled by AAA (authenticating, authorizing, and accounting) measures, including an access control list, multifactor authentication, the principle of least privilege, hard and soft tokens, smart cards, key fobs, biometric locks, digital certificates, authenticator apps, and email filtering.
- Users should be trained to detect and resist social engineering, including shoulder surfing, tailgating, dumpster diving, impersonation, phishing, email hoaxes, whaling, vishing, spear phishing, and spoofing.

Dealing with Malicious Software on Personal Computers

- Malware includes viruses, spyware, keyloggers, worms, Trojans, rootkits, boot sector viruses, ransomware, on-path attacks, zero-day attacks, DoS (denial-of-service) attacks, DDoS (distributed denial-of-service) attacks, zombies, botnets, and crypto miners. Attacks on passwords include dictionary, brute force, and rainbow table attacks.
- Vulnerability to attack is increased by noncompliant systems, unpatched systems, an OS working past its end of life, careless programming that allows for SQL injections and cross-site scripting, insider threats, and lack of user education.
- Symptoms that indicate malware is present include pop-up ads, browser redirection, desktop alerts, application crashes, failed OS updates, antivirus false alerts, slow performance, error messages and logs, file errors, email problems, and invalid digital certificates.
- Some systems become so highly infected that the only solution is to format the hard drive, reinstall Windows, and restore data from backups.
- To clean up an infected system,

    1. know how to identify common malware symptoms,
    2. quarantine the infected system,
    3. disable System Protection,
    4. remediate the system,
    5. protect the system with scheduled scans and updates,
    6. enable System Protection and create a restore point, and
    7. educate the end user.

Licensing, Regulated Data, and Security Policies

- The owner of a copyright for software has the right to allow the software to be copied and used and assign a license to do so, after the user agrees to a EULA (End User License Agreement).
- Two types of licenses for copyrighted software are a personal use license and a commercial use license. Two types of open-source licenses are a copyleft and permissive license.
- Regulatory and compliance policies help protect regulated data, which can include PII (personally identifiable information), PHI (protected health information), PCI (Payment Card Industry) data, and government-issued personal information that is regulated by governmental agencies.
- Data can be partly or completely destroyed using a low-level format, zero-fill utility, Secure Erase utility, drill, hammer, incinerator, degausser, paper shredder, or multimedia shredder.
- Professional data-destruction vendors may provide a certificate of destruction for legal purposes.

- A chain-of-custody document is part of incident documentation and provides a paper trail of the evidence in response to an incident that is suspected to be criminal.

16-4c Thinking Critically

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use information from other modules and the web.

1. An employee uses a key fob to access corporate resources from their home office. What type of authentication are they using?

    1. Mutual authentication
    2. Soft token
    3. Authenticator app
    4. SMS messaging
2. What tool is best to use when destroying data on an SSD?

    1. Zero-fill utility
    2. Low-level format
    3. Degausser
    4. ATA Secure Erase
3. What is one difference between a video surveillance camera and a webcam? Select all that apply.

    1. One camera is a part of the IoT, and the other is not.
    2. One camera is accessible from the Internet, and the other is not.
    3. One camera has an IP address, and the other does not.
    4. One camera has a lens, and the other does not.
4. What device can be installed on a laptop to prevent shoulder surfing?

    1. USB port
    2. Smart card reader
    3. Fingerprint reader
    4. Privacy filter
5. Which definition describes a virus? A Trojan?

    1. A program that can replicate by attaching itself to another program
    2. A program that can spread copies of itself throughout a network without a host program
    3. A program that does not need a host program to work; it substitutes itself for, and pretends to be, a legitimate program
    4. A program that displays ads in a web browser
6. What is the best way to determine if an email message warning about a virus is a hoax?

    1. Check websites that track virus hoaxes.
    2. Scan the message for misspelled words or grammar errors.
    3. Open the message and see what happens.

4. Scan your email inbox for malware.

7. What is the first thing you should do when you discover a computer is infected with malware? The second thing?

   1. Turn off system protection.
   2. Update installed anti-malware software.
   3. Format the hard drive.
   4. Quarantine the computer.

8. What does anti-malware software look for to determine that a program or a process is a virus?

9. What registry key keeps information about services that run when a computer is booted into Safe Mode?

10. What folder is used by Windows to hold restore points?

11. What must you do in Windows to allow anti-malware software to scan and delete malware it might find in the data storage area where restore points are kept?

12. A virus has attacked your hard drive. Instead of seeing the Windows Start screen when you start up Windows, the system freezes, and you see a blue screen of death. You have important document files on the drive that are not backed up. What do you do first? Explain why this is your first choice.

    1. Try a data-recovery service even though it is expensive.
    2. Remove the hard drive from the computer case, and install it in another computer.
    3. Try GetDataBack by Runtime Software (runtime.org) to recover the data.
    4. Use Windows utilities to attempt to fix the Windows boot problem.
    5. Run antivirus software to remove the virus.

13. You sign in to your personal computer with your Microsoft account, and you want to set up your computer as a trusted device to make changes to the account settings. Microsoft sends a code to your cell phone in a text message. You enter the code on a Windows screen. This type of authentication is called .

    1. multifactor authentication
    2. mutual authentication
    3. biometric authentication
    4. None of the answers are correct.

14. At a restaurant, you overhear people discussing an interesting case they treated while working in a dental office that day. Which type of regulated data policies are most likely to have been violated?

    1. PII
    2. PHI
    3. PCI
    4. GDPR

15. Among the following, which is the best protection against ransomware?

    1. Windows File History
    2. Carbonite

3. Keylogger software
4. Authy by Twilio

16. When you started your new job, your training included reading through the company intranet website AUP pages. This morning you see a coworker violating a policy. You ask whether they are aware that they are violating the policy, and they respond that they are aware. What is your next step?

1. Ignore the incident and wait to see whether it happens again.
2. Tell your manager about the situation.
3. Tell another coworker and ask them what you should do.
4. Ask a coworker how to fill out an incident report.

17. You sign in to your banking website on a new computer and get a request that the bank needs to send you a text code to your cell phone to authenticate the sign in. Why is this method of authentication not secure?

1. Biometric data is not being used.
2. The digital certificate for the bank's website may be outdated.
3. Multifactor authentication does not authenticate the user.
4. SMS text is not encrypted.

18. You suspect a boot sector virus has infected your computer. How can you remove the virus?

1. Perform a full scan using Microsoft Defender Antivirus.
2. Replace the hard drive.
3. Perform a Microsoft Defender Offline scan.
4. Boot the system in Safe Mode with Networking, and run Microsoft Defender Antivirus.

19. You work in the IT department of a large hospital, and your manager has asked you to dispose of several old laptops previously used by the medical staff. How do you proceed?

1. Delete all user accounts on the laptops, and donate them to a nonprofit organization.
2. Remove the hard drives from all the laptops, replace them with new hard drives, and then donate them to a nonprofit organization.
3. Physically destroy all the hard drives, and then donate the laptops to the computer repair labs at the local community college.
4. Sell the laptops on eBay.com, and donate the money to a charity of your choice.

6-4d Hands-On Projects

Hands-On Project 16-1

Using the Web to Learn About Malware

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 2.3

One source of information about malware on the web is F-Secure Corporation. Go to the website f-secure.com or another anti-malware site, and find information about the latest malware threats. Answer the following questions:

1. Which site did you use to research the latest malware?
2. Name and describe a recent Trojan downloader. How does the Trojan install, and what is its payload (the harm it does)?
3. Name and describe a recent rootkit. How does the rootkit install, and what is its payload?
4. Name a recent worm. How does it get into the network, and what is its payload?

Hands-On Project 16-2

Researching CoC and Incidence Response Documents

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 4.6

Your manager has been asked to create the documentation necessary for your new data-destruction company to be compliant when handling regulated data. They have asked you to recommend some sample documentation for chain-of-custody (CoC) and incident-response documents. Find three examples of each document. For the CoC documents, which components do each sample have in common? For the incident-response documents, which components do each sample have in common? Which CoC document would you recommend? Which incident-response document would you recommend?

Hands-On Project 16-3

Researching HIPAA Rules and Compliance

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 4.6

You have just landed your perfect next job working in the IT department of your local hospital as a systems analyst on the security team. Your new manager tells you that your first task on the job is to learn as much as you can about HIPAA. To get started, research the following topics, write a brief overview of each topic, and don't forget to cite an authoritative source (a source that is the final authority on a matter) to support your findings:

1. Two rules that generally govern HIPAA regulations are the HIPAA privacy rule and the HIPAA security rule. Briefly describe each rule.
2. List three methods that are included in the guidance for compliance for each HIPAA rule.
3. Which organization is responsible for adopting, communicating, and enforcing the national standards for the two HIPAA rules?
4. Which entities or individuals are responsible for abiding by these HIPAA rules?

Hands-On Project 16-4

Researching Disposal Rules

- **Est. Time:** 15 minutes

- **Core 2 Objective:** 4.5

Research the laws and regulations in your community concerning the disposal of batteries and old computer parts. Answer these questions:

1. How do you properly dispose of a monitor in your community?
2. How do you properly dispose of a battery pack used by a notebook computer?
3. How do you properly dispose of a large box of assorted computer parts, including hard drives, optical drives, computer cases, and circuit boards?

16-4e Real Problems, Real Solutions

Real Problem 16-1

Downloading and Using Anti-Malware Software

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 2.3

A free trial of AVG Protection software is available on the AVG site at avg.com. Do the following to download, install, and run the software:

1. 1
   Download the free trial version of AVG Protection software from avg.com and install the software.
2. 2
   Update the software with the latest malware signatures.
3. 3
   Perform a complete scan of the system. Were any suspicious programs found?
4. 4
   Verify the software is set to scan for rootkits.
5. 5
   Verify the software is set to scan incoming and outgoing email and their attachments.

Real Problem 16-2

Creating and Using an Anti-Malware Software Rescue Disk

- **Est. Time:** 45 minutes including file download time
- **Core 2 Objective:** 3.3

When an infected computer refuses to boot, one method to clean the infection is to create and use an anti-malware rescue disk. For example, the rescue disk currently offered by Kaspersky is Kaspersky Rescue Disk 18. Do the following to create a bootable USB flash drive, CD, or DVD; use it to scan a computer; and answer the following questions:

1. 1

Go to support.kaspersky.com/krd18 and get familiar with the directions to create and use the rescue disk. Download the rescue disk software. What are the name and size of the download file for the rescue disk?

2. 2
   Create a bootable USB flash drive, CD, or DVD, and then write the Kaspersky image to the boot media.
    1. Which boot media did you use?
    2. Which program did you use to make the media bootable?
3. 3
   Boot from the rescue disk. On the opening menu, highlight **English** and press **Enter**. What are the options on the next menu screen?
4. 4
   Continue the boot using the rescue disk graphic mode. Accept the EULA. Using the default parameters, is the software set to scan the Windows volume? Boot sectors? BIOS firmware?
5. 5
   Label the disk or flash drive, and save it in case you need it to remediate an infected computer.

An employee uses a key fob to access corporate resources from their home office. What type of authentication are they using?

○ a. Mutual authentication

○ b. SMS messaging

○ c. Soft token

○ d. Authenticator app

What tool is best to use when destroying data on an SSD?

○ a. Zero-fill utility

○ b. Degausser

○ c. ATA Secure Erase

○ d. Low-level format

What is one difference between a video surveillance camera and a webcam? Select all that apply.

□ a. One camera is a part of the IoT, and the other is not.

□ b. One camera is accessible from the Internet, and the other is not.

□ c. One camera has an IP address, and the other does not.

□ d. One camera has a lens, and the other does not.

What device can be installed on a laptop to prevent shoulder surfing?

○ a. Smart card reader

○ b. Privacy filter

○ c. Fingerprint reader

○ d. USB port

Which definition describes a virus?

○ a. A program that displays ads in a web browser

● b. A program that can replicate by attaching itself to another program

○ c. A program that can spread copies of itself throughout a network without a host program

○ d. A program that does not need a host program to work; it substitutes itself for, and pretends to be, a legitimate program

What is the best way to determine if an email message warning about a virus is a hoax?

○ a. Scan the message for misspelled words or grammar errors.

○ b. Open the message and see what happens.

○ c. Check websites that track virus hoaxes.

○ d. Scan your email inbox for malware.

What is the first thing you should do when you discover a computer is infected with malware?

○ a. Turn off system protection.

○ b. Update installed anti-malware software.

○ c. Format the hard drive.

○ d. Quarantine the computer.

A virus has attacked your hard drive. Instead of seeing the Windows Start screen when you start up Windows, the system freezes, and you see a blue screen of death. You have important document files on the drive that are not backed up. What do you do first?

○ a. Use Windows utilities to attempt to fix the Windows boot problem.

○ b. Try a data-recovery service even though it is expensive.

○ c. Remove the hard drive from the computer case, and install it in another computer.

○ d. Try GetDataBack by Runtime Software (*runtime.org*) to recover the data.

○ e. Run antivirus software to remove the virus.

You sign in to your personal computer with your Microsoft account, and you want to set up your computer as a trusted device to make changes to the account settings. Microsoft sends a code to your cell phone in a text message. You enter the code on a Windows screen. This type of authentication is called _________________.

○ a. multifactor authentication

○ b. mutual authentication

○ c. biometric authentication

○ d. None of the answers are correct.

At a restaurant, you overhear people discussing an interesting case they treated while working in a dental office that day. Which type of regulated data policies are most likely to have been violated?

○ a. PCI

○ b. PHI

○ c. PII

○ d. GDPR

Among the following, which is the best protection against ransomware?

○ a. Keylogger software

● b. Carbonite

○ c. Authy by Twilio

○ d. Windows File History

When you started your new job, your training included reading through the company intranet website AUP pages. This morning you see a coworker violating a policy. You ask whether they are aware that they are violating the policy, and they respond that they are aware. What is your next step?

○ a. Tell another coworker and ask them what you should do.

○ b. Ignore the incident and wait to see whether it happens again.

○ c. Ask a coworker how to fill out an incident report.

○ d. Tell your manager about the situation.

You sign in to your banking website on a new computer and get a request that the bank needs to send you a text code to your cell phone to authenticate the sign in. Why is this method of authentication not secure?

○ a. Biometric data is not being used.

○ b. Multifactor authentication does not authenticate the user.

○ c. SMS text is not encrypted.

○ d. The digital certificate for the bank's website may be outdated.

You suspect a boot sector virus has infected your computer. How can you remove the virus?

○ a. Perform a full scan using Microsoft Defender Antivirus.

○ b. Boot the system in Safe Mode with Networking, and run Microsoft Defender Antivirus.

○ c. Replace the hard drive.

○ d. Perform a Microsoft Defender Offline scan.

You work in the IT department of a large hospital, and your manager has asked you to dispose of several old laptops previously used by the medical staff. How do you proceed?

○ a. Delete all user accounts on the laptops, and donate them to a nonprofit organization.

○ b. Sell the laptops on eBay.com, and donate the money to a charity of your choice.

○ c. Remove the hard drives from all the laptops, replace them with new hard drives, and then donate them to a nonprofit organization.

○ d. Physically destroy all the hard drives, and then donate the laptops to the computer repair labs at the local community college.