Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Chapter**

**17**

**Security Strategies and Documentation**

* [Chapter Introduction](javascript://)
* **17-1**[Protecting Network Resources](javascript://)
  + **17-1a**[Physical Security and Access Controls](javascript://)
  + **17-1b**[Logical Security and Access Controls](javascript://)
  + **17-1c**[User Authentication](javascript://)
  + **17-1d**[User Education](javascript://)
* **17-2**[Dealing with Malicious Software on Personal Computers](javascript://)
  + **17-2a**[What Are We Up Against?](javascript://)
  + **17-2b**[Step-by-Step Attack Plan](javascript://)
  + **17-2c**[Step 1: Identifying and Researching Malware Symptoms](javascript://)
  + **17-2d**[Step 2: Quarantining an Infected System](javascript://)
  + **17-2e**[Step 3: Disabling System Restore](javascript://)
  + **17-2f**[Step 4: Remediating the Infected System](javascript://)
  + **17-2g**[Step 5: Protecting the System with Scheduled Scans and Updates](javascript://)
  + **17-2h**[Step 6: Enabling System Protection and Creating a Restore Point](javascript://)
  + **17-2i**[Step 7: Educating the End User](javascript://)
* **17-3**[Best Practices for Documentation and Security Policies](javascript://)
  + **17-3a**[Types of Documentation](javascript://)
  + **17-3b**[Change Management](javascript://)
  + **17-3c**[Regulated Data, Licensing, and Security Policies](javascript://)
  + **17-3d**[Data Destruction and Disposal](javascript://)
* **17-4**[Chapter Review](javascript://)
  + **17-4a**[Chapter Summary](javascript://)
  + **17-4b**[Key Terms](javascript://)
  + **17-4c**[Thinking Critically](javascript://)
  + **17-4d**[Hands-On Projects](javascript://)
  + **17-4e**[Real Problems, Real Solutions](javascript://)
  + **17-4f**[Exam Tips](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

Chapter Introduction

After completing this chapter, you will be able to:

* Explain how to secure resources on a network via physical and logical access control, user authentication, and user education
* Recognize malicious software and remove it to protect personal computers
* Describe policies that address issues of change management, regulated data, software licensing, incident response, and data destruction and disposal

In [Chapter 16](javascript://), you learned the concepts and principles of securing Windows resources on workstations and networks by classifying users and data, and you learned how to protect resources by applying appropriate permissions so that only authorized users can access the data. In this chapter, you learn about additional tools and techniques to secure the resources on a personal computer and network. You also learn how to recognize that a personal computer is infected with malware and how to clean an infected system and keep it clean. Finally, you learn what your employer might expect of you when dealing with issues of change management, regulated data, software licensing, incident response, and data destruction and disposal.

[Chapter 16](javascript://) and this chapter give you the basics of securing a personal computer or network. Later in your career as a support technician, you can build on the skills learned in these chapters to implement even more security, such as controlling how Windows stores its passwords.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**17-1**Protecting Network Resources

**A+ Core 2**

* 2.1

Summarize the importance of physical security measures.

* 2.2

Explain logical security concepts.

* 2.3

Compare and contrast wireless security protocols and authentication methods.

* 2.4

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

* 2.10

Given a scenario, configure security on SOHO wireless and wired networks.

* 4.1

Compare and contrast best practices associated with types of documentation.

In this part of the chapter, you learn both physical and logical methods of protecting computer resources, securely authenticate users on a large network, and educate users to understand their roles to protect and secure network resources by carefully following established best practices.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-1aPhysical Security and Access Controls

**A+ Core 2**

* 2.1

Summarize the importance of physical security measures.

* 2.2

Explain logical security concepts.

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:

* **If the data 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. 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 that are 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 might have written down. Door locks and safes come in several types, including keyed locks, combination locks, and biometric locks. [**Biometric locks**](javascript://) require special input called [**biometric data**](javascript://) to identify a person by her fingerprint, handprint, face, retina, iris, voice, or handwritten signature. [Figure 17-1](javascript://) shows a biometric input device: a fingerprint scanner. Many mobile devices, such as iPads and some laptops, have fingerprint scanners built in.

**Figure 17-1**

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



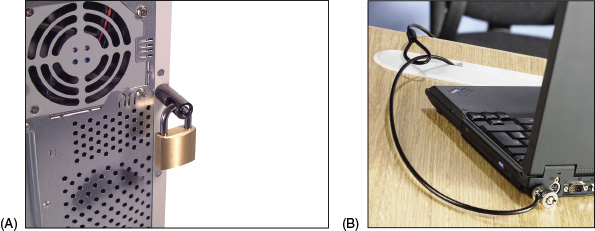
Enlarge Image

Source: [iStockphoto.com/viiwee](http://istockphoto.com/viiwee" \t "_blank)

* **Use server locks or cable locks**. Some computer cases allow you to add a lock so that you can physically prevent others from opening the case (see [Figure 17-2A](javascript://)). These locks, called [**server locks**](javascript://), might be used on computers that hold corporate data. You can also use a **cable lock**, or [**Kensington lock**](javascript://), to secure a laptop or other computer to a table so someone can’t walk away with it (see [Figure 17-2B](javascript://)). Most laptops have a security slot on the case to connect the cable lock; this slot is called a [**Kensington Security Slot**](javascript://) 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.

**Figure 17-2**

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



Enlarge Image

* **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**](javascript://) to restrict physical access to the exposed ports. The [**USB lock**](javascript://) by PadJack, Inc., consists of three pieces, as shown in [Figure 17-3](javascript://). 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 17-3**

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



Enlarge Image

Source: [PadJack.com](http://padjack.com/" \t "_blank)

* **Use privacy screens**. To keep other people from viewing a monitor screen, you can install a [**privacy screen**](javascript://), also called a [**privacy filter**](javascript://), 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 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. The numbers or barcode identify you as the owner and can clearly establish to police that the laptop has been stolen. Two sources of theft-prevention plates and cable locks are Flexguard Security System ([flexguard.com](http://flexguard.com/" \t "_blank)) and Computer Security Products, Inc. ([computersecurity.com](http://computersecurity.com/" \t "_blank)). See [Figure 17-4](javascript://). 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 inventory management system.

**Figure 17-4**

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



Source: [computersecurity.com/stop/](http://computersecurity.com/stop/" \t "_blank)

* **Use a mantrap and security guard**. The ultimate in physical security is a [**mantrap**](javascript://), 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 badge for the first door and a fingerprint scan for the second door. A security guard might also maintain an [**entry control roster**](javascript://), which is a list of people allowed into the restricted area and a log of any approved visitors.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-1bLogical Security and Access Controls

**A+ Core 2**

* 2.2

Explain logical security concepts.

* 2.10

Given a scenario, configure security on SOHO wireless and wired networks.

Software, such as Windows Firewall, can make up a significant portion of your defense resources. Other types of software-based security measures include:

* **Antivirus/anti-malware**. [**Antivirus software**](javascript://) or [**anti-malware software**](javascript://) monitors a device for activity that is recognized to be harmful to data or other resources. The software then attempts to block the activity, identify the source of the problem, and remove any malicious files that have infected the computer. You’ll learn more about viruses, malware, and antivirus/anti-malware software later in this chapter.
* **Email filtering**. Email providers often offer [**email filtering**](javascript://) 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)**](javascript://) software, which helps protect against leaking corporate data.
* **Trusted software sources**. It’s important to download software only from trusted publishers and providers. Even software from a trusted publisher can be filled with destructive extras if the software is obtained from an untrusted provider. Also know that a website might be trying to trick you into thinking you’re downloading applications, software updates, or drivers from a trusted source when you’re actually downloading malware. Be careful which sites you use for software downloads.
* **Access control lists**. An [**access control list (ACL)**](javascript://) includes which user, device, or program has access to a particular resource, such as a printer, folder, or file, on a corporate network or computer. As you learned in [Chapter 16](javascript://), larger corporate networks manage access control through Active Directory on a Windows domain, and, on smaller peer-to-peer networks, each computer controls access to its own resources. For both types of networks, Group Policy can control user rights, and NTFS permissions and share permissions control access to files and folders.
* **Port security and MAC address filtering**. Recall that a switch has multiple Ethernet ports for devices to connect to the network. See [Figure 17-5](javascript://). By default, any device can connect to any port; however, you can enable [**port security**](javascript://) to control which devices can use any port or a specific port on the switch. Most managed switches (switches that can be configured through a web-based utility) can provide **MAC address filtering**, which allows you to specify how many MAC addresses a port can accept or to provide a whitelist of MAC addresses the switch will accept. Because it’s so easy to spoof, or counterfeit, a legitimate MAC address, MAC address filtering is not considered a recommended best practice as your only layer of defense against attack.

**Figure 17-5**

This managed switch by Cisco allows for MAC address filtering on its Ethernet ports



Enlarge Image

Source: [cisco.com/c/en/us/support/switches/catalyst-2960s-48lps-l-switch/model.html](http://cisco.com/c/en/us/support/switches/catalyst-2960s-48lps-l-switch/model.html" \t "_blank)

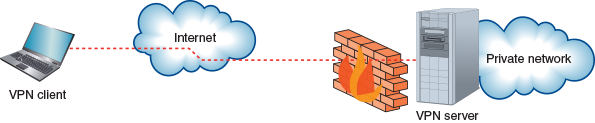
**Notes**

MAC address filtering can also be implemented on a SOHO router, and can easily be hacked as part of your defenses against attack. Therefore, MAC address filtering should only serve as one layer of defense among many. These various layers of defense are collectively called **defense in depth**.

* **VPN**. Recall from [Chapter 7](javascript://) that a **VPN (virtual private network)** protects data by encrypting it over a remote connection to a private network. When you set up a VPN, the VPN software (for example, OpenVPN at [openvpn.net](http://openvpn.net/" \t "_blank) and [privatetunnel.com](http://privatetunnel.com/" \t "_blank)) creates a virtual tunnel between the client computer and a VPN server behind the private network’s firewall. Network packets are encrypted at one end of the tunnel and decrypted as they exit the tunnel. VPN connections are used for telecommuters to securely connect to their corporate networks (see [Figure 17-6](javascript://)) or for individuals to securely surf the web. In the latter use, all transmissions are sent between the client computers and web servers through a VPN service center that manages the VPN connection. Managed switches, including the one shown earlier in [Figure 17-5](javascript://), sometimes have VPN services embedded in their firmware so they can provide VPN connections for remote users of the private network to which they belong.

**Figure 17-6**

A VPN connection secures all traffic between the VPN client and VPN server on the private network



Enlarge Image

* **Mobile device management**. Corporate or personal mobile devices present a particular set of security challenges because they hold sensitive company data while traveling outside of the company network’s physical perimeter. [**Mobile device management (MDM)**](javascript://) software provides tools for tracking mobile devices—even when they’re turned off—and managing the data on those devices. [**MDM policies**](javascript://) typically include:
  + Security policy enforcement, such as applying patches or enforcing password requirements
  + Data encryption requirements, to protect data on the mobile device even if it falls into the wrong hands
  + Remote wipe capabilities, to erase all data on the device

To do all this, MDM installs a small app called an [**agent**](javascript://) on a managed mobile device, which communicates through various Wi-Fi or cellular connections back to the MDM server in the company data center. The initial installing of the agent and the agent checking the device for security compliance is called [**on-boarding**](javascript://). The reverse process when the mobile device is removed from the MDM fleet is called [**off-boarding**](javascript://). You learned more about BYOD (Bring Your Own Device) security in a corporate environment in [Chapter 9](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-1cUser Authentication

**A+ Core 2**

* 2.2

Explain logical security concepts.

* 2.3

Compare and contrast wireless security protocols and authentication methods.

In [Chapter 16](javascript://), you learned that the first line of defense to protect a network is user authentication. Besides Windows authenticating a user with a Windows password, you can increase authentication security using these methods:

* Enforce a [**password policy**](javascript://), which is a set of rules that defines the minimum length of a password, complexity requirements, and how frequently a password must be reset, for example.
* Enforce **multifactor authentication**, which requires at least one more factor or action to authenticate beyond the single-factor password. [**Two-factor authentication (2FA)**](javascript://) is most often used, and the two factors normally involve what the user:
  + Knows (such as a Windows or Facebook password)
  + Possesses, which is called a token (such as a smart card or key fob)
  + Does (such as typing a certain way)
  + Is, which is called biometric data (such as a fingerprint)

One warning to keep in mind is that factors such as a smart card or biometric data should be used in addition to, and not as a replacement for, a Windows password on a personal computer or domain.

Next, let’s look at hardware and software security tokens and authentication services that can work together to provide multifactor authentication.

### Hardware Security Tokens

Two types of hardware security tokens are a smart card and a key fob:

* **Smart card**. A [**smart card**](javascript://) used as a security token has an embedded microprocessor, which is 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**](javascript://) when the device is inserted into the reader or transmitted wirelessly. See [Figure 17-7](javascript://). At the same time, most smart cards can receive information from the card reader to confirm that the reader is authentic. This is called [**mutual authentication**](javascript://), which occurs when authentication goes in both directions at the same time and both entities confirm the identity of the other. Because a smart card contains a microprocessor and data, it’s considered both a hardware token and a software token.

**Figure 17-7**

A smart card is read by a wireless smart card reader



Source: [istock.com/humonia](http://istock.com/humonia" \t "_blank)

**Notes**

A common use of mutual authentication is sending a confirmation code by text to your smartphone using a phone number the server already has on file. This gives you reassurance that the server to which you’re authenticating is what it says it is.

* **Key fob**. A [**key fob**](javascript://) is a hardware token that fits conveniently on a keychain, such as the one shown in [Figure 17-8](javascript://). The number on the key fob changes every 60 seconds. When a user signs in to the network, he must enter the number on the key fob, which 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 17-8**

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



Source: [iStockphoto.com](http://istockphoto.com/" \t "_blank)/David Clark

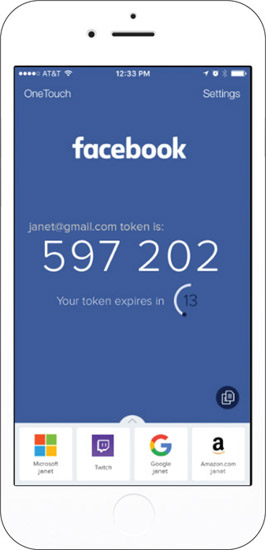
### Software Security Tokens

[**Software tokens**](javascript://) can be security tokens stored as an app or digital certificate. Here’s how each works:

* **Software token apps**. These apps, sometimes called authenticator apps, are installed on your smartphone or other computing device and can perform the same service as a key fob, providing a counter or number generator that serves as one factor in multifactor authentication. The app is synchronized with the same calculations on the server so that the app and the server expect the same number at the same time. Software token providers for 2FA include Google Authenticator ([google.com](http://google.com/" \t "_blank)), Twilio Authy ([authy.com](http://authy.com/" \t "_blank)), and LastPass Authenticator ([lastpass.com/auth](http://lastpass.com/auth" \t "_blank)). 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 17-9](javascript://)).

**Figure 17-9**

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



Enlarge Image

Source: [https://authy.com/features/setup/](https://authy.com/features/setup/" \t "_blank) by Twilio, Inc.

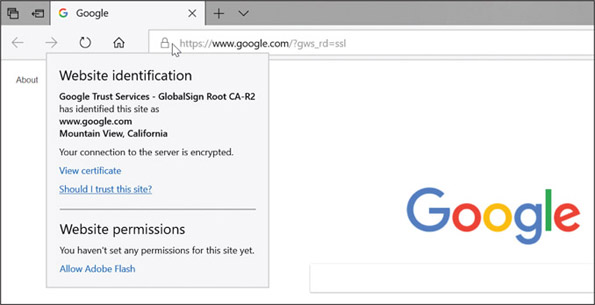
In general, to set up 2FA with an online account, you would:

* 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.
* **Digital certificates**. Think of a [**digital certificate**](javascript://) 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, and is similar to a notary verifying that a signature is legitimate. The digital certificate and public encryption key are assigned by a [**Certificate Authority (CA)**](javascript://) that has confirmed your identity in a separate process. VeriSign ([verisign.com](http://verisign.com/" \t "_blank)) and GlobalSign ([globalsign.com](http://globalsign.com/" \t "_blank)) are two 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 and then click the lock icon, as shown in [Figure 17-10](javascript://). Click **View certificate**.

**Figure 17-10**

Google’s digital certificate is provided by GlobalSign, Inc.



Enlarge Image

Source: [google.com](http://google.com/" \t "_blank)

### Authentication Services

For large networks, you learned in [Chapter 16](javascript://) that Active Directory on a Windows domain is used to authenticate users to the domain and authorize what users can do with domain resources. For added security, everything users attempt to do or do once they are authenticated to the network can be tracked or logged for future auditing. These three security measures are generally known in networking as [**AAA (authenticating, authorizing, and accounting)**](javascript://) or [**triple A**](javascript://). Two popular solutions to provide AAA services for large networks are RADIUS and TACACS+:

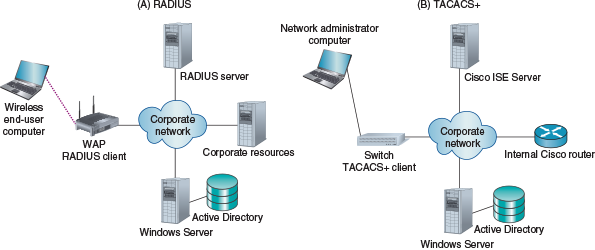
* [**RADIUS (Remote Access Dial-In User Service)**](javascript://) was originally developed to authenticate end users accessing resources on a network through dial-up connections and has evolved to other types of connections to a network, including wired, wireless, and VPN.
* [**TACACS+ (Terminal Access Controller Access Control System Plus)**](javascript://) was developed by Cisco to improve on RADIUS for AAA services specifically designed for network administrators and technicians to remotely connect to a network to configure and manage Cisco network devices, such as routers, switches, and firewalls.

RADIUS and TACACS+ each can work with Active Directory or some other type of directory server to authenticate and authorize users, and sometimes both services are used on the same network. RADIUS and TACACS+ can each support wireless, wired, and VPN connections. Notice in [Figure 17-11](javascript://) the similarities of how each service works; both use a client, server, and user directory:

* **Client**. A RADIUS or TACACS+ client can be a wireless access point (WAP) or switch that receives the initial connection from the user’s laptop or other device. The client is responsible for querying the RADIUS or TACACS+ server to authenticate the user before allowing the user on the network.
* **Server**. A RADIUS or TACACS+ server authenticates the user by querying a user directory. Cisco calls its TACACS+ server the Identify Service Engine server (ISE server).
* **User directory**. The RADIUS to ISE server queries a user directory or database, where user credentials are stored. Active Directory is the most popular user directory for today’s large networks.

**Figure 17-11**

AAA services provided by (A) RADIUS and (B) TACACS+ protocols and services



Enlarge Image

**Notes**

Often, a basic WAP isn’t smart enough to act as the RADIUS or TACACS+ client. In an enterprise environment, many WAPs are connected to a wireless controller device in the data closet, which in turn does the work of managing client requests to the RADIUS or ISE server.

In summary, [Table 17-1](javascript://) compares RADIUS and TACACS+.

**Table 17-1**

### RADIUS and TACACS+ Characteristics

| **Characteristic** | **RADIUS** | **TACACS+** |
| --- | --- | --- |
| Primary use | Intended for end-user network access | Intended for Cisco network device administrative access |
| Encryption | Encrypts user passwords only | Encrypts every message |
| Underlying protocol | The RADIUS protocol uses UDP, which does not guarantee transmissions over the corporate network | The TACACS+ protocol uses TCP to guarantee transmissions over the corporate network |
| Network types | Works on wireless, wired, and VPN network connections | Works on wireless, wired, and VPN network connections |

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-1dUser Education

**A+ Core 2**

* 2.4

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

* 2.5

Compare and contrast social engineering, threats, and vulnerabilities.

* 4.1

Compare and contrast best practices associated with types of documentation.

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. 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**](javascript://) is the practice of tricking people into giving out private information or allowing unsafe programs into the 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. A document that can help educate users is an [**acceptable use policy (AUP)**](javascript://), which explains what users can and cannot do on the corporate network or with company data, and explains the penalties for violations. The AUP might also describe how these measures help protect the network’s security. Important security measures that users need to follow to protect passwords and the computer system are:

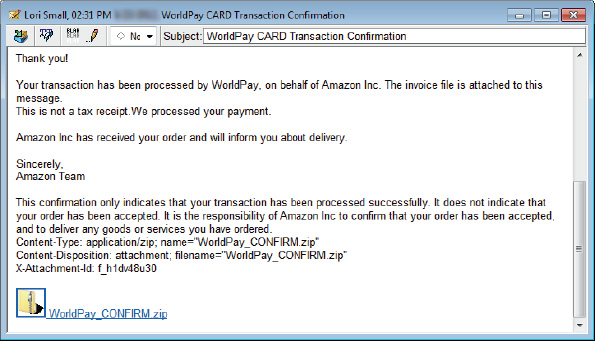
* Never give out your passwords to anyone, not even a supervisor or tech support person who calls and asks for it.
* Don’t store your passwords on a computer unless you use company-approved password vault software (for example, KeePass or LastPass). Some organizations even forbid employees from writing down their passwords.
* Don’t use the same password on more than one computer, network, application, or website.
* Be aware of [**shoulder surfing**](javascript://), which is when other people secretly peek at your monitor screen as you work. A privacy filter can help.
* Lock down your workstation each time you step away from your desk.
* Users need to be on the alert for [**tailgating**](javascript://), which is when an unauthorized person follows an employee through a secured entrance to a room or building. Another form of tailgating is when a user steps away from a computer that’s not properly locked and another person continues to use the Windows session.

Hackers might obtain information or trick people into giving information that can be used to hack a computer or network by:

* **Dumpster diving**. [**Dumpster diving**](javascript://) is looking for useful information in someone’s trash to help create a convincing [**impersonation**](javascript://) 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, spear phishing, impersonation, and spoofing**. [**Phishing**](javascript://) (pronounced “fishing”) is a type of identity theft in which the sender of an [**email hoax**](javascript://) scams you into responding with personal data about yourself. Even more plausible is [**spear phishing**](javascript://), where the 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**](javascript://), which means the scam artist makes both the email and website look like the real thing. For example, when the user who received the email shown in [Figure 17-12](javascript://) scanned the attached file using antivirus software, the software reported that the file contained malware.

**Figure 17-12**

This phishing technique using an email message with an attached file is an example of social engineering



Enlarge Image

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:

* [snopes.com](http://snopes.com/" \t "_blank) by Barbara and David Mikkelson

* [securelist.com](http://securelist.com/" \t "_blank) by Kaspersky Lab

* [virusbtn.com](http://virusbtn.com/" \t "_blank) by Virus Bulletin, Ltd

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!

**Notes**

A helpful tool to combat phishing attacks is a [**Secure DNS**](javascript://) service (sometimes written as SecureDNS), which monitors requests for websites and redirects your browser when it attempts to visit a known malicious site. Popular providers include the free SecureDNS service by Comodo ([comodo.com](http://comodo.com/" \t "_blank)) and the enterprise-grade SecureDNS service by RiskAnalytics ([riskanalytics.com](http://riskanalytics.com/" \t "_blank)). To use Secure DNS on a personal computer, go to the Network Connections window, open the active connection’s TCP/IPv4 properties box, and change the DNS server settings so your computer uses Secure DNS server addresses listed on the provider’s website.

**A+ 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 tailgating, phishing, spear phishing, impersonation, shoulder surfing, and dumpster diving.

A study by Dell showed that 65 percent of business travelers have not secured the corporate data on their hard drives, and 42 percent don’t back up that data. Here are some commonsense rules to help protect a laptop when traveling:

* When traveling, always know where your laptop is. If you’re standing at an airport counter, tuck your laptop case securely between your ankles. At security checkpoints, pay attention to your belongings; tell yourself to stay focused. When flying, never check your laptop as baggage, and don’t store it in airplane overhead bins; keep it at your feet.
* Never leave a laptop in an unlocked car. If you leave your laptop in a hotel room, use a laptop cable lock to secure it to a table.
* When at work, lock your laptop in a secure place or use a laptop cable lock to secure it to your desk.

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

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**17-2**Dealing with Malicious Software on Personal Computers

**A+ Core 2**

* 2.4

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

* 2.5

Compare and contrast social engineering, threats, and vulnerabilities.

* 3.2

Given a scenario, troubleshoot and resolve PC security issues.

* 3.3

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

[**Malicious software**](javascript://), also called [**malware**](javascript://), is any unwanted program that is intended for harm and is transmitted to your computer without your knowledge. [**Grayware**](javascript://) 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 part of the chapter, 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.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2aWhat Are We Up Against?

**A+ Core 2**

* 2.4

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

* 2.5

Compare and contrast social engineering, threats, and vulnerabilities.

* 3.2

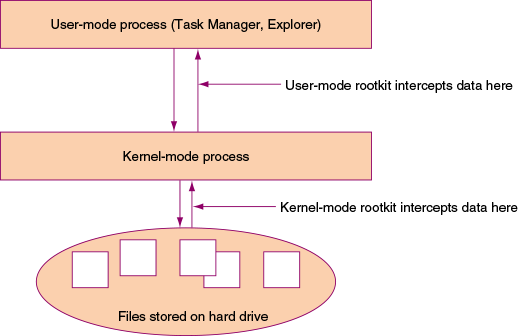
Given a scenario, troubleshoot and resolve PC security issues.

You need to know your enemy! In 2017, it was reported that more than 8 million new malware programs were discovered. Different categories of malware and scamming techniques are listed next:

* **Viruses**. A [**virus**](javascript://) 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**](javascript://) spies on you to collect personal information that it transmits over the Internet to web-hosting sites. An example of spyware is a [**keylogger**](javascript://) 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**](javascript://) 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**](javascript://) does not need a host program to work; rather, it substitutes itself for a legitimate program. In most cases, a user launches it thinking she is 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 (refer back to [Figure 17-12](javascript://)).
* **Rootkits**. A [**rootkit**](javascript://) 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 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 17-13](javascript://)).

**Figure 17-13**

A rootkit can run in user mode or kernel mode



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 Windows tools and components to work, the rootkit is not detected or cannot be deleted if the Windows 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 Windows.

* **Ransomware**. [**Ransomware**](javascript://) holds your computer system hostage until you pay money. For example, the CryptoLocker Trojan program that did damage in 2014 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 File Explorer. 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](http://carbonite.com/" \t "_blank)), Backblaze ([backblaze.com](http://backblaze.com/" \t "_blank)), or IDrive ([idrive.com](http://idrive.com/" \t "_blank)). After a ransomware attack, you can wipe the computer, reinstall software from original sources, and restore unaffected file versions from your online backups.

* **Zero-day attack**. A [**zero-day attack**](javascript://) 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 and fourth Tuesday of each month (known as patch Tuesday), but sometimes releases patches off schedule so that hackers have less time to attack customers.
* **Man-in-the-middle attack**. In a [**man-in-the-middle attack**](javascript://), 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 an “evil twin” Wi-Fi hotspot, 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 man-in-the-middle attacks is to use digital certificates to identify a person or service before transmitting sensitive information.
* **Denial of service**. A [**denial-of-service (DoS)**](javascript://) attack overwhelms a computer or network with requests or traffic until new connections can no longer be accepted. A [**distributed denial-of-service (DDoS)**](javascript://) attack happens when multiple computers are involved in the attack. DDoS attacks are sometimes performed by botnets, which are described next.
* **Zombies and botnets**. A [**zombie**](javascript://) 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**](javascript://) (a network of robots). The CryptoLocker Trojan program was distributed by a botnet and ultimately isolated when the botnet was taken down.
* **Dictionary attack**. A [**dictionary attack**](javascript://) can be used to crack a password by trying words in a dictionary. Password cracker software might combine a [**brute force**](javascript://) 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**](javascript://) 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 a hacker obtains a stolen list of hashed passwords, she can compare this list with those in her rainbow tables to find a match. When two hashed passwords match, she 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).

* **Noncompliant systems and violations of security best practices**. A system administrator needs techniques in place to routinely scan BYOD and corporate-owned smartphones, tablets, laptops, desktops, and servers for [**noncompliant systems**](javascript://) that violate security best practices, such as out-of-date anti-malware software or cases where it’s not installed. One software product designed to scan devices for noncompliance is System Center Configuration Manager by Microsoft, which works with Microsoft Intune. Intune focuses specifically on mobile devices that connect to a corporate network.

**A+ Exam Tip**

The A+ Core 2 exam might give you a scenario that requires you to detect, remove, or prevent viruses, Trojans, worms, spyware, keyloggers, ransomware, rootkits, and botnet software. You also need to identify and describe zero-day attacks, man-in-the-middle attacks, zombies, dictionary attacks, brute force attacks, phishing, spear phishing, impersonation, shoulder surfing, tailgating, dumpster diving, DoS/DDoS attacks, rainbow tables, spoofing, and noncompliant systems.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2bStep-by-Step Attack Plan

**A+ Core 2**

* 3.3

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

This section is 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 system, you can try a repair upgrade, a fresh start, or a reset without losing user data. For Windows 8, a refresh can be an excellent option if you have a recent custom refresh image. For Windows 7, consider applying a system image. In [Chapter 15](javascript://), you learned about all of these options to reinstall Windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2cStep 1: Identifying and Researching Malware Symptoms

**A+ Core 2**

* 3.3

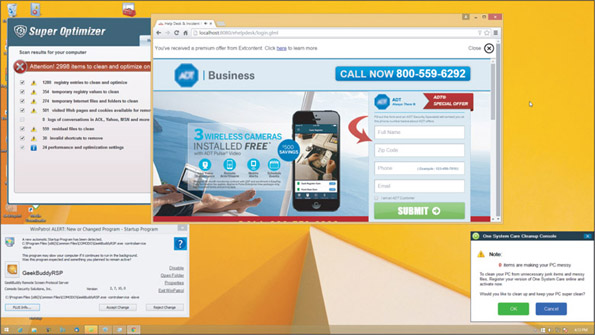
Given a scenario, use best practice procedures for malware removal.

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 and browser redirection**. Basically, a user is losing control of his system. For example, [Figure 17-14](javascript://) shows the desktop immediately after a user signed in. Pop-up ads are randomly appearing and the browser home page has changed. A browser might also have an uninvited toolbar. Security alerts—real or spoofed—regularly interrupt the user’s activity.

**Figure 17-14**

A hijacked home page, security alerts, and pop-up ads indicate an infected system



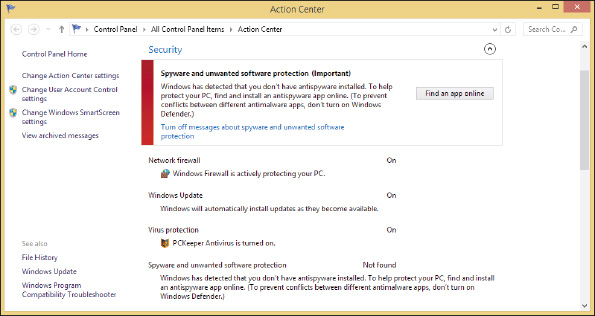
Enlarge Image

Source: Ruiware, LLC

* **Rogue antivirus software**. When the user tries to run Windows Defender (anti-malware software embedded in Windows 8), it refuses to run. She opens the Action Center to find that Defender has been disabled because other antivirus software she did not install is running. See [Figure 17-15](javascript://).

**Figure 17-15**

Action Center reports Windows Defender has been disabled and rogue antivirus software is running



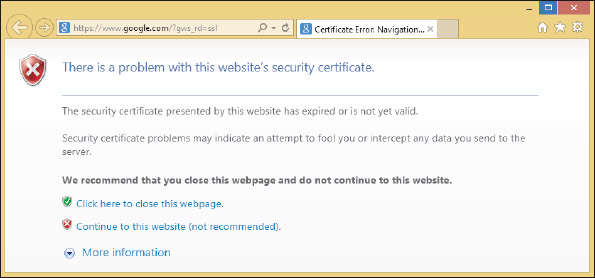
Enlarge Image

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 Windows Defender.

* **Slow performance or lockups**. 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.
* **Internet connectivity issues, 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.
* **System and application log errors**. The Administrative Events logs in Event Viewer report system and application errors, system crashes, application crashes, and failed OS updates.
* **Problems with files**. File names now have weird characters 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.
* **Email problems**. You receive email messages from other users saying you have sent someone spam or an infected message, or you receive automated replies indicating you sent email you didn’t know about. This type of attack indicates that your email address or email client software on your computer has been hijacked. Extra spam you’re not accustomed to seeing shows up.
* **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](http://symantec.com/" \t "_blank) or [mcafee.com](http://mcafee.com/" \t "_blank), and you cannot update your anti-malware software.
* **Invalid digital certificates**. 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**](javascript://) 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 17-16](javascript://)). Don’t trust websites or email whose certificates have expired or been revoked.

**Figure 17-16**

Windows reports a problem with a digital certificate



Enlarge Image

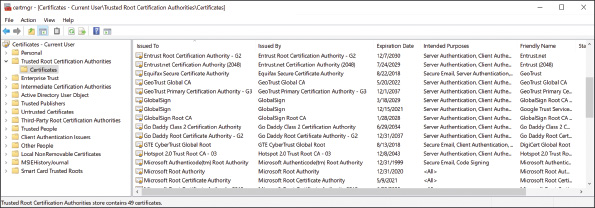
**Notes**

If a computer gives invalid certificate errors, 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](http://certmgr.msc/" \t "_blank)) to view and delete root certificates, as shown in [Figure 17-17](javascript://). For example, the Superfish virus injects a rogue root certificate into the Microsoft store of trusted certificates on the local computer so that it can perform a man-in-the-middle 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 17-17**

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



Enlarge Image

**A+ 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 know how to quarantine and remediate an infected system.

**Notes**

Malicious software is designed to do varying degrees of damage to data and software, although 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.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2dStep 2: Quarantining an Infected System

**A+ Core 2**

* 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**](javascript://) 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.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2eStep 3: Disabling System Restore

**A+ Core 2**

* 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 that anti-malware software can clean the System Volume Information folder (see [Figure 17-18](javascript://)). 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.

**Figure 17-18**

Malware found in a restore point



Source: McAfee VirusScan

**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.

To turn off System Protection, go to **Control Panel**, open the **System** window, and 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.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2fStep 4: Remediating the Infected System

**A+ Core 2**

* 3.3

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

[Table 17-2](javascript://) lists popular anti-malware software for personal computers and the programs’ 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.

**Table 17-2**

### Anti-Malware Software and Websites

| **Anti-Malware Software** | **Website** |
| --- | --- |
| Maximum, Internet, or Antivirus+ Security by Trend Micro (for home use) | [trendmicro.com](http://trendmicro.com/" \t "_blank) |
| Avast Ultimate, Premium, or Free Antivirus (for home use) | [avast.com](http://avast.com/" \t "_blank) |
| Bitdefender Antivirus Plus, Internet Security, or Total Security | [bitdefender.com](http://bitdefender.com/" \t "_blank) |
| ClamWin Free Antivirus (open source and free) | [clamwin.com](http://clamwin.com/" \t "_blank) |
| F-Secure Total, Safe, Anti-Virus, or Online Scanner (Online Scanner is free) | [f-secure.com](http://f-secure.com/" \t "_blank) |
| Kaspersky Internet Security, Anti-Virus, or Security Cloud (Security Cloud is free) | [kaspersky.com](http://kaspersky.com/" \t "_blank) |
| Malwarebytes for Windows (free version available) | [malwarebytes.com](http://malwarebytes.com/" \t "_blank) |
| McAfee Total Protection | [mcafee.com](http://mcafee.com/" \t "_blank) |
| Symantec Endpoint Protection | [symantec.com](http://symantec.com/" \t "_blank) |
| Panda Dome Essential, Advanced, or Complete | [pandasecurity.com](http://pandasecurity.com/" \t "_blank) |
| SUPERAntiSpyware (free edition available) | [superantispyware.com](http://superantispyware.com/" \t "_blank) |
| Windows Defender (included in Windows 10/8), Microsoft Security Essentials (free for Windows 7) | [microsoft.com](http://microsoft.com/" \t "_blank) |

**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.

**Notes**

[**Windows Defender**](javascript://) anti-malware software is embedded in Windows 10/8 and can be accessed through the Windows 10 Settings app or Windows 8 Control Panel. Windows 7 includes Windows Defender, but the Windows 7 version finds only spyware, not viruses and other malware. For Windows 7, you can download and install Microsoft Security Essentials, which is free anti-malware software.

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

### 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. [Chapter 15](javascript://) 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.

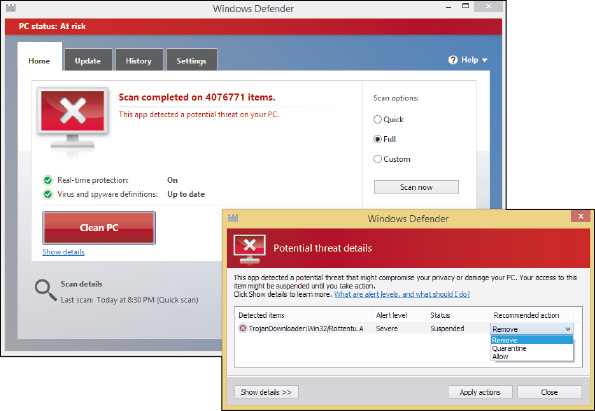
### Update and Run Anti-Malware Software That’s Already Installed

If anti-malware software is already installed on a system and you suspect an infection, update the software and perform a full scan on the system. Do the following:

1. Make sure the anti-malware software is up to date. These updates download the latest [**malware definitions**](javascript://), also called [**malware signatures**](javascript://), which the software uses to define or detect new malware as it gets into the wild (becomes available on the Internet).
2. Use the anti-malware software to perform a full scan of the system. As it scans, the software might ask you what to do with an infected program, or it might log the event in an event viewer or history log it keeps. For example, Windows Defender reports a threat, as shown in [Figure 17-19](javascript://). When you click **Clean PC**, you can decide what to do with the threat. In most situations, select **Remove** to delete the program.

**Figure 17-19**

Decide what to do with a program that Windows Defender has identified as a severe threat to the system



Enlarge Image

1. 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.

**Notes**

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.

### Run Anti-Malware Software from a Networked Computer

If anti-malware software is not already installed, the most effective way to clean the computer is to run the software from another computer. Follow these steps:

1. 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.
2. Network the two computers and share drive C: on the infected computer. (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.)
3. To make your work easier, you can map a network drive from the remote computer to drive C: on the infected computer.
4. Perform an anti-malware scan on the remote computer, pointing the scan to drive C: on the infected computer.

### Install and Run Anti-Malware Software on the Infected Computer

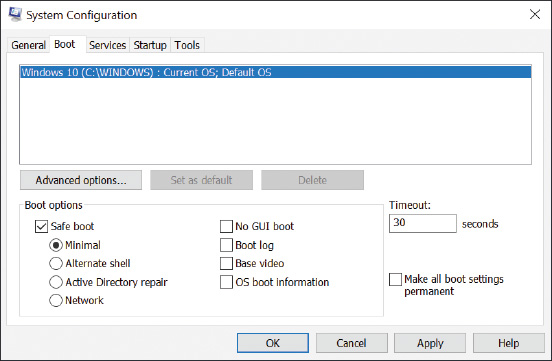
If you don’t have another computer that you are willing to risk connecting to the infected computer, you can use another computer to purchase and download anti-malware software and then copy the downloaded files to a CD or flash drive that you can insert in the infected computer. Don’t make the mistake of using the infected computer to purchase and download anti-malware software because keyloggers might be spying and collecting credit card information. During the installation process, the anti-malware software updates itself and performs a scan. You can also run free online anti-malware software without downloading and installing it, but be careful to use only reputable websites.

### Install and Run Anti-Malware Software in Safe Mode

Some malware prevents anti-malware software from installing or running. In this situation, try booting the system in Safe Mode or performing a clean boot and installing the anti-malware software. Some viruses still load in Safe Mode or after a clean boot, and some anti-malware programs will not install in Safe Mode. Recall that to launch Windows in Safe Mode, also called Safe boot, enter the **msconfig** command in the Windows 10/7 search box or the Windows 8 Run box. In the System Configuration box, click the **Boot** tab and check **Safe boot** (see [Figure 17-20](javascript://)). To launch Safe Mode with Networking so that you can update your anti-malware software, select **Network** in the list of options. Then restart the system.

**Figure 17-20**

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



**Notes**

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 [Chapter 14](javascript://).

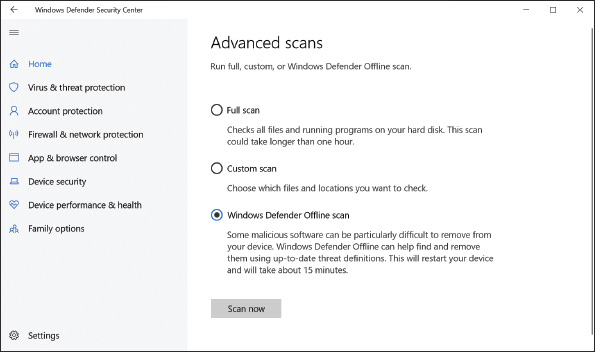
### Run an Anti-Malware Scan before Windows Boots

Microsoft offers a specialized scanning utility called [**Windows Defender Offline (WDO)**](javascript://) that loads before Windows and performs a scan in the **Windows Preinstallation Environment (WinPE)**. WinPE is a limited version of Windows that can be used for customizing Windows installations, modifying the Windows installation while it’s not running, or performing recovery tasks. WDO can be started from the Windows 10 Settings app:

1. Click **Update & Security**, **Windows Security**, and **Virus & threat protection**.
2. In the Windows Defender Security Center window that opens, click **Run a new advanced scan**. Select **Windows Defender Offline scan**, as shown in [Figure 17-21](javascript://). Make sure all apps and files are saved and closed, then click **Scan now**.

**Figure 17-21**

A WDO scan searches for and removes malware in the Windows Preinstallation Environment



Enlarge Image

1. After the scan completes, find information about the scan in the Virus & threat protection window by clicking **Threat history**.

If you’re unable to boot into Windows 10, or if you’re working with an earlier version of Windows, use an uninfected computer to create a bootable CD or flash drive with the WDO tool, and then boot from that device:

1. Depending on the architecture of the infected machine, download the 32-bit or 64-bit version of WDO from the Microsoft support website at the following link and save it to a CD or flash drive:

* + [support.microsoft.com/en-us/help/17466/windows-defender-offline-help-protect-my-pc](http://support.microsoft.com/en-us/help/17466/windows-defender-offline-help-protect-my-pc" \t "_blank)

1. Boot from the WDO device, perform the scan, and check the results.

Other anti-malware companies, such as those listed in [Table 17-2](javascript://), offer preinstallation scanning tools, also called rescue disks or bootable antivirus tools. Two examples are the Bitdefender Rescue CD ([bitdefender.com](http://bitdefender.com/" \t "_blank)) and Kaspersky’s Rescue Disk ([kaspersky.com](http://kaspersky.com/" \t "_blank)).

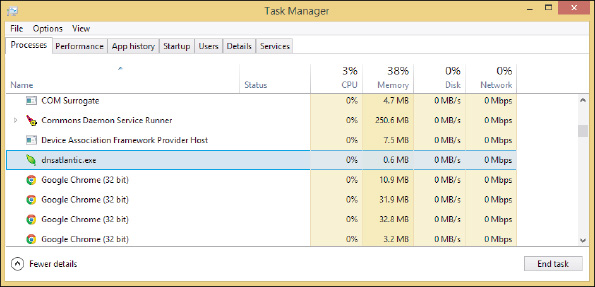
### Run More than One Scan of Anti-Malware Software

After you’ve scanned the system using one of the methods just discussed, reboot and install anti-malware software on the hard drive. 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, Windows Defender 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 17-22](javascript://)).

**Figure 17-22**

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



Enlarge Image

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](http://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download" \t "_blank)) is not designed for ongoing malware prevention but can sometimes remove malware that Windows Defender 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 System Configuration and/or 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 [Chapter 14](javascript://) for the details of how to remove unwanted startup programs.
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. Also, Task Manager and other tools might find processes you suspect are malware. The web is your best tool to use when making your decision about a program. Here are some websites that offer [**malware encyclopedias**](javascript://) that are reliable and give you symptoms and solutions for malware:
   * Process Library by ProcessLibrary at [processlibrary.com](http://processlibrary.com/" \t "_blank)
   * DLL Library by Uniblue Systems Limited at [liutilities.com](http://liutilities.com/" \t "_blank)
   * All the anti-malware software sites listed earlier in the chapter in [Table 17-2](javascript://)

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.

1. **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:
   * First try File Explorer or Windows Explorer to locate a file and delete it. For peace of mind, don’t forget to empty the Recycle Bin when you’re done.
   * If the file is hidden or access is denied, open an elevated command prompt window and use the commands listed in [Table 17-3](javascript://) 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 17-3**

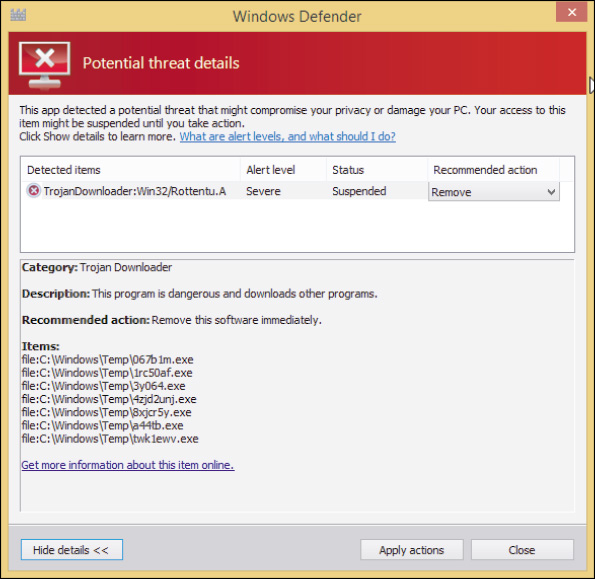
### Commands Used to Take Control of a Malware File so You Can Delete It

|  |  |
| --- | --- |
| **Command** | **Description** |
| attrib –r –s filename.ext | Remove the read-only and system attributes to a file. |
| tasklist | more  taskkill /f /pid:9999 | To stop a running process, first use the tasklist command to find out the process ID for the process. Then use the taskkill command to forcefully kill the process with the given process ID. |
| takeown /f filename.ext | Take ownership of a file. |
| icacls filename.ext /grant administrators:f | Take full access of a file. |

* + To get rid of other malware files, delete all Internet Explorer temporary Internet files. Use the Disk Cleanup process in the Drive C: properties box, or delete the browsing history using the Internet Options box.
  + Delete all subfolders and files in the C:\Windows\Temp folder. [Figure 17-23](javascript://) shows where Windows Defender lists potentially unwanted programs (PuPs) that a Trojan downloader put in this folder.

**Figure 17-23**

A Trojan downloader put programs in the C:/Windows/Temp folder, which must be manually deleted

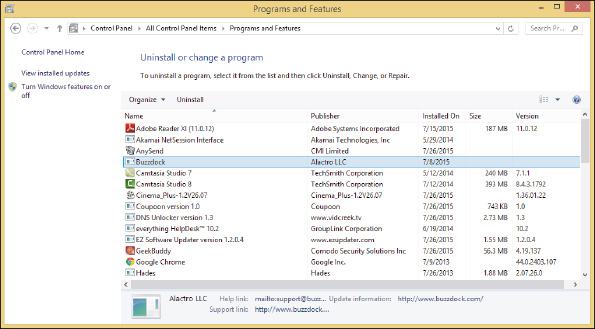


Enlarge Image

1. **Clean the registry.** Appendix B lists folders and registry keys that can affect startup. You can search these folders and keys and delete entries you don’t want. After you have finished cleaning startup folders and the registry, don’t forget to restart the system and make sure all is well before you move on.
2. **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. [Chapter 16](javascript://) covered how to use the Internet Options 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 (see [Figure 17-24](javascript://)).

**Figure 17-24**

A Trojan downloader installed several unwanted programs, which must be uninstalled



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2gStep 5: Protecting the System with Scheduled Scans and Updates

**A+ Core 2**

* 3.3

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

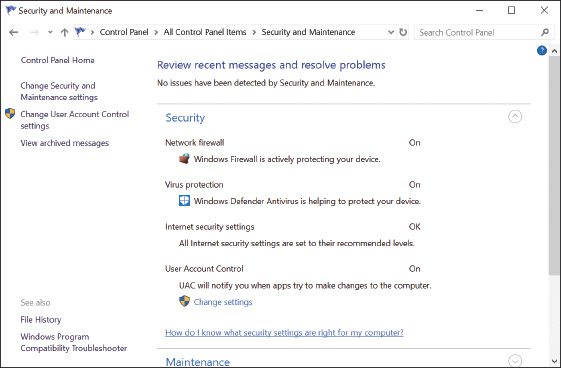
Once your system is clean, you’ll certainly want to keep it that way. The three best practices to protect a system against malware are:

* **Use anti-malware software.** Install and run anti-malware software and keep it current. Configure the software so that 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.

To find out what anti-malware software is installed and turned on, open the Windows 10 Security and Maintenance window in Control Panel (see [Figure 17-25](javascript://)).

**Figure 17-25**

Check which apps are providing security protections for your computer



**OS Differences**

In Windows 8/7, open the Action Center to see what anti-malware software is installed and running.

* **Always use a software firewall.** Never, ever connect your computer to an unprotected network without using a firewall. Windows Firewall is turned on by default. Recall that you can configure Windows Firewall to allow no uninvited communication or to allow the exceptions that you specify.
* **Keep Windows updates current.** Microsoft continually releases updates to plug vulnerable entrances in Windows where malware might attack and updates to Windows Defender and Microsoft Security Essentials. Recall that you can verify Windows Update settings in the Settings app (Windows 10 only) or by clicking **Windows Update** in the System window in Control Panel (Windows 8/7).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2hStep 6: Enabling System Protection and Creating a Restore Point

**A+ Core 2**

* 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 [Chapter 13](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-2iStep 7: Educating the End User

**A+ Core 2**

* 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 chapter 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.

**A+ 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.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**17-3**Best Practices for Documentation and Security Policies

**A+ Core 2**

* 2.9

Given a scenario, implement appropriate data destruction and disposal methods.

* 4.1

Compare and contrast best practices associated with types of documentation.

* 4.2

Given a scenario, implement basic change management best practices.

* 4.6

Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.

Well-run IT departments rely on good documentation and security policies to set expectations and standards for security in the entire organization. In this part of the chapter, you learn about the types of documentation and security policies you might encounter in your IT career and what is generally expected of you as an IT technician to follow these best practices and policies.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-3aTypes of Documentation

**A+ Core 2**

* 4.1

Compare and contrast best practices associated with types of documentation.

Earlier in this text, you learned about ticketing software that tracks, manages, and documents customer service in an IT organization, acceptable use policies (AUP) that document what users can and cannot do with corporate resources, and password policies that document how to create strong passwords. Other types of documentation and documentation software an IT technician might encounter in an organization are described next:

* **Knowledge base.** A [**knowledge base**](javascript://) is a collection of articles containing text, images, or video that give information about a network, product, or service. Here are two examples of how a knowledge base might be used:
  + **Customer service.** To better support customers, a company might publish a knowledge base about its products or services on its website. Technical support specialists usually have access to a knowledge base to aid in helping customers during support calls; the knowledge base might be integrated into a ticketing system.
  + **IT training and troubleshooting.** As IT personnel install, configure, and troubleshoot devices and software, the information they learn can be documented in the IT department’s knowledge base so it’s readily available for future troubleshooting and for training new IT personnel.
* **Inventory management.** [**Inventory management**](javascript://) documents inventory, including end-user devices, network devices, IP addresses, software licenses, and related licenses. Hardware inventory might track equipment by using asset tags and theft-prevention plates, as you learned earlier in the chapter. These tags and plates contain [**barcodes**](javascript://) that are easily read by a laser scanner. See [Figure 17-26](javascript://). Asset tracking software can scan the barcodes to report on existing inventory, track equipment, report needed maintenance, and help with identifying and returning stolen property.

**Figure 17-26**

The print on this tag is embedded under a protective surface so it can’t be easily damaged

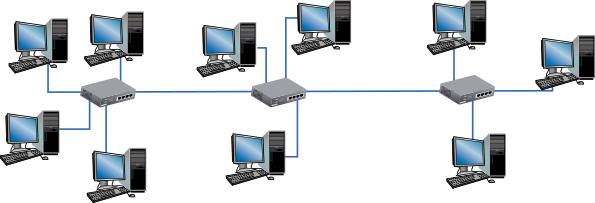


Source: [MyAssetTag.com](http://myassettag.com/" \t "_blank)

* **Password policy.** In [Chapter 16](javascript://), you learned what is required to create a strong password and best practices for passwords (for example, allowing one to expire so that the user must occasionally change it). These requirements are sometimes documented as a password policy.
* **Network topology diagrams.** Network documentation should contain a map of a network’s topology, which is called a [**network topology diagram**](javascript://). In networking, [**topology**](javascript://) refers to the pattern in which devices on a network are connected with each other. For example, devices connected in a line are using a bus topology, and devices connected to a single, centralized device are using a star topology. Recall from [Chapter 8](javascript://) that most Ethernet networks today use a design called a star bus topology, which means that nodes are connected to one or more centralized devices that are connected to each other (see [Figure 17-27](javascript://)).

**Figure 17-27**

A star bus network formed by nodes connected to multiple switches



Enlarge Image

A network topology diagram might show how nodes on a network are physically connected, such as the one in [Figure 17-27](javascript://), or it might show the logical network topology. For example, the diagram shown earlier in [Figure 17-11](javascript://) shows the logical connection among clients and servers to indicate how data flows among them.

On small networks, a network topology diagram can be hand drawn, but for larger networks, inventory data is usually compiled automatically through network scans. For example, Spiceworks ([spiceworks.com](http://spiceworks.com/" \t "_blank)) offers a free Network Inventory product that probes devices on the network and presents a list of detected devices along with any information gathered about them, such as IP addresses, installed operating systems, and shared folders.

You learn about other types of documentation, such as that involved with change management, later in this chapter.

**A+ Exam Tip**

The A+ Core 2 exam requires you to understand the similarities and differences between various types of documentation, including network topology diagrams, knowledge base articles, incident documentation, regulatory and compliance policies, acceptable use policies, and inventory management documentation. All are discussed in this chapter.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-3bChange Management

**A+ Core 2**

* 4.2

Given a scenario, implement basic change management best practices.

As an IT support technician, you will undoubtedly be involved in new projects, such as installing hardware or software, upgrading networks, moving IT operations from onsite services to cloud-based services, rolling out virtualized desktops across the organization, implementing a VoIP communication platform, and much more. A project is temporary—it has a beginning, an end, and a singular, well-defined goal. A successful project depends on expert project management to direct a project team through specific tasks and deliver results on time, within the agreed-to budget, and with complete customer satisfaction.

When a project is implemented, change happens. Change managed well means that people affected by the change can make a smooth transition from their current state to the project goal or end result. In most situations, [**change management**](javascript://) is closely integrated with project management and often involves the same teams. For example, a project manager works with a team to plan, develop, test, and implement new software. A change manager might work with the same team to define how the software will affect people and manage all communication, scheduling, training, and support required so that affected people are satisfied, embracing and accepting the end result.

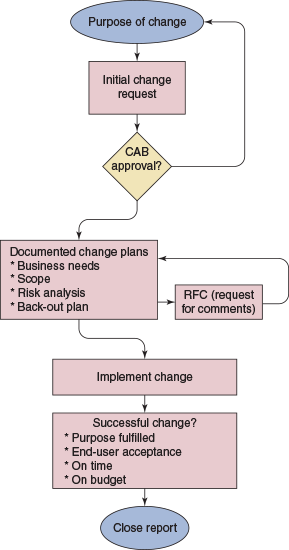
**A+ Exam Tip**

The A+ Core 2 exam will give you a scenario and expect you to apply the basic principles of change management, including documenting business processes, purpose of change, scope of change, risk analysis, end-user acceptance, change boards, back-out plans, and the need to document change.

A high-level change process is diagrammed in [Figure 17-28](javascript://). Know, however, that change processes vary widely. Let’s look at the basic elements of change management and how they might relate to you as an IT support technician.

**Figure 17-28**

The general flow of change management



Enlarge Image

### Documented Business Processes

A business is complex and well-run organizations know they must understand and document their core business goals and processes. [**Documented business processes**](javascript://) are related activities that lead to a desired business goal, such as an efficient and cost-effective service, excellent customer satisfaction, or a superior product. For example, if customer satisfaction is a defined business goal, IT operational processes might describe how customers are taken care of, support tickets are documented, and customer satisfaction is measured.

As change happens, be aware of how this change affects documented business processes. For example, suppose help-desk software is changed so that the customer’s electronic signature is required when a ticket is closed. If you forget the electronic signature, your company may not be able to collect payment or follow up with the customer for a satisfaction survey.

### Purpose of Change

The starting point for every proposed change is a clear and concise purpose for the change. What will change? What is the current situation and expected outcome? Why is the change needed? What happens if the organization does not initiate this change? How will the success of the change be measured?

**Notes**

IT technicians often communicate with people impacted by change. Therefore, it’s important that you have a firm understanding of the purpose for the change so that you can maintain a positive, helpful attitude.

A proposed change is formally submitted using a change request process. A change request states what needs to be updated or changed but does not indicate how the change will be executed. A simple change request might require only preapproval from a manager. Complex changes, with higher impact and risks, are submitted to a change advisory board. The [**change advisory board (CAB)**](javascript://) meets on a regular basis to assess, prioritize, authorize, and schedule changes. The change manager and other representatives approve changes based on the recommendations of the change advisory board.

### Change Plan and Scope

The change plan defines the [**scope of change**](javascript://), which may outline:

* Key components of the change and how they will be addressed
* Skill sets, tasks, and activities required to carry out the change
* Individuals or departments that will participate in the change
* How the success of change is measured and when the change is completed

The scope of change defines your responsibilities in the change plan. It’s important that you understand exactly your assignment for planning, implementing, and supporting the change and then work within these boundaries, which is called working “in scope.” The scope of change might evolve through the feedback process of change management, but until the scope changes, it’s important to work in scope. Although it might be tempting to perform yet one more step while implementing a change, don’t make “out of scope” modifications, which might result in major disruption.

### Risk Analysis

Change almost always involves risk, which refers to a problem (event, situation, or condition) that may or may not occur as a result of the change. For example, a change might be half-finished when the change manager realizes the budget is inadequate. Other risks are alienating customers, not finishing on time, or not delivering the intended results. [**Risk analysis**](javascript://) is the process of identifying potential problems so there are no surprises or crisis situations once the change begins. For each potential problem identified, the team attempts to determine the likelihood it may occur, its impact, and what to do if it does occur. As an IT technician, you need to be aware of the risks involved and how to execute the response plan if the problem actually happens.

### Back-Out Plan

What if a change goes bad—really bad? Suppose all users lose network connectivity for hours or all database servers that log all online sales orders spontaneously crash. The [**back-out plan**](javascript://) defines the activities needed to recover to the original state in the event of an aborted or failed change implementation. The back-out plan is created and sometimes tested even before the change starts, and includes detailed steps to restore service to users. Obviously, you need to be aware of the back-out plan prior to implementing a change.

### End-User Acceptance

Recall that change management is responsible for people impacted by change being able to make a smooth transition during the change. End-user acceptance to change often fails because the focus of the change is on the technical side rather than the people side. To gain end-user acceptance, users must know:

1. The purpose of the change, especially the business reasons for the change
2. That the leadership of the company agrees with the change
3. How the change will affect them and their job
4. How to get their individual concerns and questions answered and how their voices will be heard
5. That they will receive end-user training for the changes that impact them

Before a change begins, an organization might request user feedback to the change in a [**request for comments (RFC)**](javascript://). Technical users often have valuable input in the RFC process that may affect the entire change process. IT technicians often play a major role in end-user acceptance. Users who struggle with change will appreciate your empathetic and positive outlook. When a proposed change has been clearly communicated and the user understands “what’s in it for me,” you have made a significant contribution to a successful change.

### Document Changes

No part of change management should rely on spoken communication. Everything related to changes must be documented, including how the change management process itself works. Change plans are documented and updated throughout the entire change management process. Many larger organizations use change management software, such as Alloy Software ([alloy-software.com](http://alloy-software.com/" \t "_blank)), to manage all stages of change management from the change request form to the final close report. Smaller organizations may manually document change using MS Word or Excel documents or database software. Regardless of the size of the organization, you will be expected to maintain proper documentation for all stages of a change in which you participate.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-3cRegulated Data, Licensing, and Security Policies

**A+ Core 2**

* 4.1

Compare and contrast best practices associated with types of documentation.

* 4.2

Given a scenario, implement basic change management best practices.

* 4.6

Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.

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

### Regulatory and Compliance Policies

Certain types of data are protected by special governmental regulations and are called [**regulated data**](javascript://). Each industry must comply with a variety of regulations, policies, and laws, which are collectively called [**regulatory and compliance policies**](javascript://). For example, in the health-care 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 regulated industries include the 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.

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

* **Personal identity**. [**PII (personally identifiable information)**](javascript://) is a legal term to describe data that can uniquely identify a person, including a Social Security number, email address, physical address, birthdate, birth place, 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.
* **Health information**. [**PHI (protected health information)**](javascript://) 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)**](javascript://) 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 transmitted (such as when receiving payments) and stored (such as when keeping records for recurring billing) by vendors, retailers, and financial institutions.
* **Citizens of the EU**. The [**GDPR (General Data Protection Regulation)**](javascript://) is a group of regulations implemented in 2018 in the European Union (EU) to protect personal data of EU citizens, giving them more control over how their data is collected, stored, and shared. The GDPR also includes requirements for how individuals should be notified in the event their data is hacked. Covered personal data includes name, address, photos, IP address, genetic information, and biometric data that uniquely identifies a person.

**Notes**

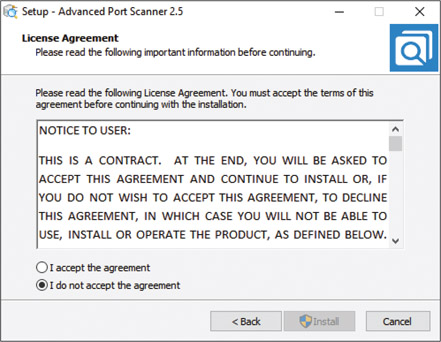
Organizations and individuals who have access to regulated data are at risk legally and financially if they do not comply with the legal requirements regarding the security of this data. When you work in an organization that handles regulated data, ensure your own protection by making certain you understand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

### Software Licensing

As an IT support technician, you need to be especially aware of the issues surrounding software licensing. As you have learned, open source software can be freely distributed and installed, but closed source software is owned by the creator (developer) and a license is required to use the software. When someone purchases software from a software developer, that person or organization has only purchased a **commercial 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. The right to copy the work, called a [**copyright**](javascript://), 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. Your rights to use or copy software are clearly stated in the [**End User License Agreement (EULA)**](javascript://) that you agree to when you install the software (see [Figure 17-29](javascript://)).

**Figure 17-29**

Agreeing to the EULA is required before software installs



Source: Famatech Corp.

Making unauthorized copies of original software violates the Federal Copyright Act of 1976 and is called [**software piracy**](javascript://) 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.

**Notes**

When an individual or organization purchases the right to install one instance of software, the license is called a [**personal license**](javascript://). By purchasing a [**site license**](javascript://), also called an [**enterprise license**](javascript://), a company can obtain the right to multiple installations of software.

Many software companies, including Microsoft, have implemented measures to control the use of their software, which is called [**digital rights management (DRM)**](javascript://). For example, recall that the retail release of Windows 10 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.

### Incident Response for Prohibited Content and Activities

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**](javascript://) 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**](javascript://). If you’re the first person to discover an incident, such as use of prohibited content or other activities, you’re responsible to perform certain [**first response**](javascript://) duties. 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? 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?
* **Incident documentation**. [**Incident documentation**](javascript://) 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**](javascript://) 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. It also 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 that 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.

**A+ 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, preserving relevant data and evidence, and tracking evidence through an appropriate chain-of-custody document.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 17-3dData Destruction and Disposal

**A+ Core 2**

* 2.9

Given a scenario, implement appropriate data destruction and disposal methods.

Besides dumpster diving, consider the impact of digital dumpster diving. You need to totally destroy data before you throw out a hard drive, flash drive, CD, DVD, tape, or other media that might have personal or corporate data on it, unless you know the data can’t be stolen off the device. Trying to wipe a drive clean by deleting files or even by using Windows to format 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. With older magnetic hard drives, an end user could perform a [**low-level format**](javascript://) of a drive to redefine the sector marks on the drive’s platters, making the existing data inaccessible. (This is different from a standard Windows format that configures a file system on the drive.) Today’s devices receive a low-level format at the factory that can’t be changed later. However, end users can wipe the drive using a [**zero-fill utility**](javascript://) 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.

**Notes**

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**](javascript://) 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**](javascript://) exposes a storage device to a strong electromagnetic field to completely erase the data on a magnetic hard drive or tape drive (see [Figure 17-30](javascript://)). A degaussed drive can’t be reused, 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 17-30**

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



* **Use a shredder**. Recall you can use a paper [**shredder**](javascript://) to destroy all documents that contain sensitive data. The best paper shredders apply multiple passes to cross-cut 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**](javascript://) can also destroy optical discs. [**Disk drive shredders**](javascript://), such as the one shown in [Figure 17-31](javascript://) from Whitaker Brothers ([whitakerbrothers.com](http://whitakerbrothers.com/" \t "_blank)), can destroy magnetic hard drives, solid-state drives, flash drives, optical discs, and even mobile devices such as smartphones or small tablets.

**Figure 17-31**

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



Enlarge Image

Source: [whitakerbrothers.com](http://whitakerbrothers.com/" \t "_blank)

* **Use a secure data-destruction service**. For the very best data destruction, consider a secure data-destruction service. To find a 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**](javascript://), 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.

**A+ 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).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 17-4a**Chapter Summary**

### Protecting Network Resources

* Physical security can include a locked door, a server lock and cable lock, port lock, privacy filter, theft-prevention plate, mantrap, and security guard.
* Logical security can include anti-malware software, a VPN connection, email filtering, qualifying software distributors, an access control list, MAC address filtering, and mobile device management.
* Large networks might require additional user authentication other than a Windows password, which can include a password policy and multifactor authentication using hardware or software tokens.
* AAA (authenticating, authorizing, and accounting) services include RADIUS and TACACS+.
* Security methods include educating users against social engineering and protecting a laptop when traveling.

### Dealing with Malicious Software on Personal Computers

* Malware includes viruses, spyware, keyloggers, worms, Trojans, rootkits, ransomware, zero-day attacks, man-in-the-middle attacks, DoS attacks, DDoS attacks, zombies, and botnets. Attacks on passwords include dictionary, brute force, and rainbow table attacks. Noncompliant systems open a network up to attack.
* Symptoms that indicate malware is present include pop-up ads, 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 Restore,
  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.

### Best Practices for Documentation and Security Policies

* Types of security documentation include ticketing software to document customer service, a knowledge base, acceptable use policies, password policies, inventory management, network topology diagrams, and the documentation needed for change management.
* Change management includes identifying the purpose and scope of change, developing a change plan and back-out plan, getting approval from a change board, acquiring end-user acceptance, performing a risk analysis, and documenting the entire change process.
* Regulatory and compliance policies help protect regulated data, which can include PII, PHI, PCI, and GDPR data regulated by governmental agencies.
* Commercial licensing of software can be a personal license or enterprise license. Terms of the licensing agreement are found in the EULA.
* 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.
* Data can be partly or completely destroyed using a paper shredder, multimedia shredder, low-level format, zero-fill utility, drill, hammer, incinerator, or degausser.
* Professional data destruction services may provide a certificate of destruction for legal purposes.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 17-4b**Key Terms**

For explanations of key terms, see the Glossary for this text.

* [**AAA (authenticating, authorizing, and accounting)**](javascript://)
* [**acceptable use policy (AUP)**](javascript://)
* [**access control list (ACL)**](javascript://)
* [**agent**](javascript://)
* [**anti-malware software**](javascript://)
* [**antivirus software**](javascript://)
* [**ATA Secure Erase**](javascript://)
* [**back-out plan**](javascript://)
* [**badge reader**](javascript://)
* [**barcode**](javascript://)
* [**biometric data**](javascript://)
* **biometric lock**
* [**botnet**](javascript://)
* [**brute force**](javascript://)
* **cable lock**
* [**Certificate Authority (CA)**](javascript://)
* [**certificate of destruction**](javascript://)
* [**chain of custody**](javascript://)
* [**change advisory board (CAB)**](javascript://)
* [**change management**](javascript://)
* **commercial license**
* [**copyright**](javascript://)
* [**data loss prevention (DLP)**](javascript://)
* **defense in depth**
* [**degausser**](javascript://)
* [**denial-of-service (DoS)**](javascript://)
* [**dictionary attack**](javascript://)
* [**digital certificate**](javascript://)
* [**digital rights management (DRM)**](javascript://)
* [**disk drive shredders**](javascript://)
* [**distributed denial-of-service (DDoS)**](javascript://)
* [**documented business processes**](javascript://)
* [**dumpster diving**](javascript://)
* [**email filtering**](javascript://)
* [**email hoax**](javascript://)
* [**End User License Agreement (EULA)**](javascript://)
* [**enterprise license**](javascript://)
* [**entry control roster**](javascript://)
* [**first response**](javascript://)
* [**GDPR (General Data Protection Regulation)**](javascript://)
* [**grayware**](javascript://)
* [**impersonation**](javascript://)
* [**incident**](javascript://)
* [**incident documentation**](javascript://)
* [**incident response**](javascript://)
* [**inventory management**](javascript://)
* [**Kensington lock**](javascript://)
* [**Kensington Security Slot**](javascript://)
* [**key fob**](javascript://)
* [**keylogger**](javascript://)
* [**knowledge base**](javascript://)
* [**low-level format**](javascript://)
* **MAC address filtering**
* [**malicious software**](javascript://)
* [**malware**](javascript://)
* [**malware definitions**](javascript://)
* [**malware encyclopedias**](javascript://)
* [**malware signatures**](javascript://)
* [**man-in-the-middle attack**](javascript://)
* [**mantrap**](javascript://)
* [**MDM policies**](javascript://)
* [**mobile device management (MDM)**](javascript://)
* **multifactor authentication**
* [**multimedia shredders**](javascript://)
* [**mutual authentication**](javascript://)
* [**network topology diagram**](javascript://)
* [**noncompliant systems**](javascript://)
* [**off-boarding**](javascript://)
* [**on-boarding**](javascript://)
* [**password policy**](javascript://)
* [**Payment Card Industry (PCI)**](javascript://)
* [**personal license**](javascript://)
* [**PHI (protected health information)**](javascript://)
* [**phishing**](javascript://)
* [**PII (personally identifiable information)**](javascript://)
* [**port lock**](javascript://)
* [**port security**](javascript://)
* [**privacy filter**](javascript://)
* [**privacy screen**](javascript://)
* [**quarantined computer**](javascript://)
* [**RADIUS (Remote Access Dial-In User Service)**](javascript://)
* [**rainbow table**](javascript://)
* [**ransomware**](javascript://)
* [**regulated data**](javascript://)
* [**regulatory and compliance policies**](javascript://)
* [**request for comments (RFC)**](javascript://)
* [**risk analysis**](javascript://)
* [**root certificate**](javascript://)
* [**rootkit**](javascript://)
* [**scope of change**](javascript://)
* [**Secure DNS**](javascript://)
* [**server lock**](javascript://)
* [**shoulder surfing**](javascript://)
* [**shredder**](javascript://)
* [**site license**](javascript://)
* [**smart card**](javascript://)
* **smart card reader**
* [**social engineering**](javascript://)
* [**software piracy**](javascript://)
* [**software token**](javascript://)
* [**spear phishing**](javascript://)
* [**spoofing**](javascript://)
* [**spyware**](javascript://)
* [**TACACS+ (Terminal Access Controller Access Control System Plus)**](javascript://)
* [**tailgating**](javascript://)
* [**topology**](javascript://)
* [**triple A**](javascript://)
* [**Trojan**](javascript://)
* [**two-factor authentication (2FA)**](javascript://)
* [**USB lock**](javascript://)
* [**virus**](javascript://)
* **VPN (virtual private network)**
* [**Windows Defender**](javascript://)
* [**Windows Defender Offline (WDO)**](javascript://)
* **Windows Preinstallation Environment (WinPE)**
* [**worm**](javascript://)
* [**zero-day attack**](javascript://)
* [**zero-fill utility**](javascript://)
* [**zombie**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 17-4c**Thinking Critically**

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

1. Why is PINE963$&apple not a strong password?
2. What type of employee badge does not have to be swiped by a card reader in order to allow the employee through a door?
   1. RFID badge
   2. Smart card badge
   3. A badge containing a digital certificate
   4. Key fob
3. 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
4. What device can be installed on a laptop to prevent shoulder surfing?
5. Define and explain the differences between a virus, worm, and Trojan.
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 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 and you cannot afford to lose. 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](http://runtime.org/" \t "_blank)) 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 then 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 above
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. As a bank employee, you often work from home and remotely access a file server on the bank’s network to correct errors in financial data. Which of the following services is most likely the one you are using to authenticate to the network and track what you do on the network?
    1. RADIUS
    2. Secure DNS
    3. Active Directory
    4. TACACS+
16. Among the following, which is the best protection against ransomware?
    1. Windows File History
    2. Carbonite
    3. Keylogger software
    4. Authy by Twilio
17. Your boss asks you to work through the weekend to install new software on the applications server that serves up applications to 20 users. The following Monday, all users report they cannot open their data files. After speaking with technical support for the new application, you discover it is not compatible with the old data files. Which type of documentation should you refer to first to address this problem?
    1. Risk analysis documents
    2. Back-out plan documents
    3. Change management documents
    4. Scope of change documents

Go to pg.

[**help**](javascript://)