CHAPTER 26

Recognizing Malware and Other Threats

It's rare for any of today's computers to never access the Internet, and the Internet is a dangerous place. An unprotected computer will quickly become infected with one or more of the many types of malicious software. However, it isn't that hard to keep a computer protected. You can usually find reliable free software to protect your systems, and when a system becomes infected, there are some simple steps you can take to clean it. Beyond the digital security methods used to protect systems, there are also several physical security methods that provide an additional layer of protection.

Exam 220-802 objectives in this chapter:

- 1.7 Perform preventive maintenance procedures using appropriate tools.
  - Best practices
    - Antivirus updates
- 2.1 Apply and use common prevention methods.
  - Physical security
    - Tailgating
    - Securing physical documents/passwords/shredding
    - Privacy filters
  - Digital security
    - Antivirus
    - Antispyware
- 2.2 Compare and contrast common security threats.
  - Social engineering
  - Malware
  - Rootkits
  - Phishing
  - Shoulder surfing
  - Spyware

- Viruses
  - Worms
  - Trojans
- 2.3 Implement security best practices to secure a workstation.
  - Disable autorun
- 4.6 Given a scenario, troubleshoot operating system problems with appropriate tools.
  - Common symptoms
    - Spontaneous shutdown/restart
- 4.7 Given a scenario, troubleshoot common security issues with appropriate tools and best practices.
  - Common symptoms
    - Pop-ups
    - Browser redirection
    - Security alerts
    - Slow performance
    - Internet connectivity issues
    - PC locks up
    - Windows updates failures
    - Rogue antivirus
    - Spam
    - Renamed system files
    - Files disappearing
    - File permission changes
    - Hijacked email
    - Access denied
  - Tools
    - Anti-virus software
    - Anti-malware software
    - Anti-spyware software
    - Recovery console
    - System restore
    - Pre-installation environments
    - Event viewer
  - Best practices for malware removal
    - Identify malware symptoms

- Quarantine infected system
- Disable system restore
- Remediate infected systems: Update anti-virus software, Scan and removal techniques (safe mode, pre-installation environment)
- Schedule scans and updates
- Enable system restore and create restore point
- Educate end user

REAL WORLD **SECURITY LESSONS—THE EASY WAY AND THE HARD WAY**

Criminals have become very proficient at tricking people and separating them from their money. I recently worked with a business owner who almost lost $10,000 after falling prey to a criminal's tactics.

The owner received an official-looking email from his bank explaining a problem that urged him to verify some information to avoid losing access to his account. While the owner was normally tech-savvy, this email came to him at the end of a long problem-solving day, and he wearily looked at it as another problem he needed to solve. He clicked, logged on, and provided some other information.

What he didn't realize right away was that this was a phishing email and that he was providing information to a criminal. A little voice nagged at him that something didn't seem right, and he ended up calling the bank the next afternoon as a follow-up.

He learned three things. First, the email was not from his bank and his account did not have any problems. Second, someone withdrew almost $10,000 from his account. Third, if he didn't report this within three business days, the money from this business account would not be retrievable. (You have more time with personal accounts.) Thankfully, he reported it in time and did not lose the money.

He later explained to me what happened and asked what additional steps could be taken to prevent similar problems. I was able to help him increase both digital and physical security for his business, but what I found interesting was that he wasn't receptive to these recommendations before. I was reminded of how some lessons are learned easily while others are learned the hard way—such as after almost losing $10,000. This chapter has some important information that can help you avoid losses before they occur.

Exploring Malware

Malicious software (malware) is software with malicious intent. Many criminals write malware to infect systems for personal gain. In some cases, the malware can gather information about users to steal their identity or to access their bank accounts. Other times, a criminal wants to remotely take over the computer. Sometimes the malware will simply cause damage to the computer, making it unbootable or unusable.

EXAM TIP

Some people use the term *virus* when they're talking about any type of malware. This isn't technically accurate. When preparing for the A+ exams, you should have a good understanding of the different types of malware, such as viruses, worms, and Trojan horses.

Historically, malware has been designed to cause damage to a user's computer by deleting files or corrupting data. Sometimes it just harmlessly displayed a message like "Legalize Marijuana" and disappeared.

However, criminals have found they can make money with malware, and this has become the bigger threat. That is, today's malware usually doesn't damage the computer so that it's unusable. Often, the modifications aren't even detectable by a regular user. Instead, the malware infects the system so that the criminal can use it to steal money.

One of the biggest ways criminals make money with malware is with botnets.

Botnets

The term *botnet* is short for *robot network*. It implies a group of computers acting together on a network to perform certain tasks. Within the context of malware, a botnet is a group of computers that work together as zombies to do the bidding of a *bot herder*. Some terms related to botnets are:

- **Bot herder.** A criminal who controls a botnet. The bot herder manages one or more command and control servers and sends commands to all the computers in the botnet.
- **Command and control server.** The command and control server hosts software that can communicate with members of the botnet. The bot herder manages the command and control server.
- **Zombies.** Computers in the botnet are called *zombies* or sometimes just *bots*. They periodically check in with the command and control server. Just like a zombie in the movies, these bot zombies will do whatever they are directed to do. This often includes downloading and installing additional malware.

Bot herders sometimes rent out access to their botnet to other criminals. Malware from the other criminals can direct the zombies to send spam email to others, start attacks, or participate in other malicious actions. In many cases, the command and control server downloads remote control software. This gives the bot herder full access to the user's computer from a remote location over the Internet.

Botnets are huge. It's not uncommon for a botnet to include tens of thousands of zombie computers. Several botnets have included more than a million computers.

User's systems often join a botnet after becoming infected with malware. If antivirus (AV) software doesn't detect the infection, the users won't know. However, one sign of a botnet infection is unusual network activity when a user is not accessing the Internet.

NOTE **MALWARE DOESN'T DAMAGE ZOMBIES**

Malware installed on zombies usually doesn't cause damage for the zombie. The bot herder wants the zombie to continue to function for as long as possible. If the zombie fails, it is one less bot in the bot herder's botnet. The exception is when the bot herder is stealing money directly from the user. After accessing financial account information and cleaning out bank accounts, the criminal will often destroy the user's system to slow down any discovery.

Virus

A *virus* is malicious code that attaches itself to another host file, similar to how a flu virus attaches itself to a cell of a person. When a file is infected, the malicious code runs when the file is executed.

This provides an important distinction for a virus: it must have a host file to run. Viruses come in many forms, including the following:

- **Program or application.** It infects the executable application file, and when the file is run, the virus runs.
- **Boot sector.** It infects the boot sector of the hard drive and loads when the computer is booted.
- **Polymorphic.** The virus morphs, or changes, to prevent detection from AV software.
- **Stealth.** The virus uses different methods to hide itself from AV software.
- **Multipartite.** A multipartite virus has several components. For example, it can include elements that infect applications and the boot sector.

Viruses can infect files on just about any type of media. This includes disk drives (internal and external), USB flash drives, writable optical drives (CDs and DVDs), and tapes.

Consider the following scenario as an example of how a virus can infect a system and spread to other computers. This scenario assumes that the users are not running antivirus software with up to date definitions.

1. Mark visits a malicious website, and his system is infected with a virus. Mark doesn't know his system is infected.
2. Lori asks for a copy of a file from Mark and gives Mark her USB flash drive. As soon as Mark inserts the USB flash drive, his system detects the new hardware and infects Lori's USB flash drive with the virus.
3. Lori inserts the USB flash drive into her system. When her system accesses the USB, the virus infects Lori's system.
4. Kim asks for a file from Lori and gives Lori her USB flash drive. It infects Lori's USB flash drive, and then later Lori's system, and on and on.

A virus will usually have three goals: replicate, activate, and take action. It will try to replicate by infecting other files and other systems. At some point, it will activate to achieve an objective. It rarely activates immediately, to ensure that the virus has time to replicate. After it activates, it takes some type of action. It might join a botnet, grant an attacker remote access to the infected system, or do anything else the attacker codes into the virus.

EXAM TIP

Up to date AV software and secure settings on computers can prevent many of these infections. However, if security on systems is weakened and they are not running AV software, any of these actions can spread the virus.

Worm

A *worm* is malware that does not need a host file to run. Instead, it travels over the network by using network protocols and attempts to infect systems running specific services or applications.

EXAM TIP

A primary difference between a virus and a worm is that a worm self-replicates without user interaction. A virus requires a host file and is run after some type of user interaction.

Trojan Horse

A *Trojan horse* (sometimes called simply a *Trojan*) is malicious code that looks like something useful or fun but that is actually something else. It will often look harmless, but it can cause damage.

For example, a user might download a free registry scanner, thinking they are getting a tool that can make their system run quicker. However, when they install and run the scanner, it also runs the malicious code. It will often install a separate virus on the user's system. Even if the user later decides to uninstall the original software, the virus remains.

EXAM TIP

It's common for pirated software offered for free to actually be a Trojan horse. Users think they're getting a full version of software for free, and that might be true. However, they're often getting a little something extra. It could be a keylogger, which records their keystrokes and sends it to a criminal, or a remote access program that gives a criminal full access to their computer.

Rogueware

Rogueware (also called *rogue antivirus*, *scareware* or *ransomware*) is a form of a Trojan horse. Here's how it works.

A user visits a website and sees a pop-up window indicating that the user's computer is infected. In other cases, the webpage displays a button or a link to "free" software to scan the user's system. It then encourages the user to download and install the free software. If the user downloads and installs it, the free software "detects" viruses or other issues.

The software often includes a button or link to "clean the computer" or "remove viruses." If the user clicks the button, the rogueware then tells the user that the free version won't fix the problems. However, for only $69.95 (or some other price), the user can upgrade to the full version with all the capabilities.

In addition to getting the initial $69.95, criminals often use or sell the credit information for fraudulent charges. They are reportedly making over $30 million a month with this! As if this isn't enough, the rogueware often installs other malicious code as a Trojan horse.

IMPORTANT **ROGUEWARE CAN COME DISGUISED AS A FRIEND**

Security Essentials is a well-known rogueware program. This is not the free Microsoft Security Essentials program, but the criminals have developed it to look similar to the Microsoft one. If you want Microsoft Security Essentials, ensure that you get it from the Microsoft.com site.

Figure 26-1 shows a valid alert from Microsoft Security Essentials. Some of the error messages from rogueware will look similar. The big difference is that Microsoft Security Essentials won't charge you to clean the virus. Click the Apply Actions button in Microsoft Security Essentials, and the virus will be gone.

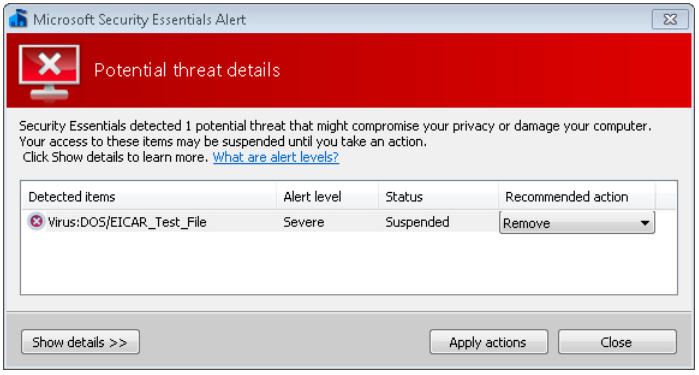


FIGURE 26-1 Microsoft Security Essentials on Windows 7.

Rootkits

A *rootkit* is a special type of malware that takes over root or administrative access on a computer. After it is installed, it can hide its presence. It controls what a user and antivirus software can view, making the rootkit difficult to detect and remove.

Antivirus software applications often include statements indicating that they can detect and remove rootkits. Unfortunately, malicious rootkits often require extraordinary measures to remove them. For example, one rootkit infects the master boot record (MBR) of a disk and write-protects it. Even if you try to reformat the disk, the virus protects the MBR and the rootkit remains present.

Spyware

Spyware is software that installs itself on the user's system, or modifies the system, without the user's knowledge or consent. The purpose is often to gain information about the user and the user's habits.

In some cases, the spyware will collect data and periodically send it back to a server on the Internet. For example, it can send a list of websites visited by the user after retrieving the list from the web browser history.

EXAM TIP

Spyware often modifies the user's web browser settings. It sometimes changes the user's home page, and other times it installs web browser add-ins or toolbar helpers. Legitimate software can do this as well, but it prompts the user before doing so.

Adware is sometimes referred to as spyware. It observes system activity and presents targeted advertisements to users. In many cases, the adware displays unwanted pop-up windows with advertisements. It can target the advertisements based on information gained about the user.

Spam and Malware

Spam is unwanted or unsolicited email. Email programs include a junk email folder and will automatically move suspected email into this folder. If you're getting spam from a specific sender, you can add the sender's email to a junk email sender list. This causes all that sender's email to be automatically moved to the junk mail folder.

While spam isn't malware itself, it is often used to deliver malware or to trick a user into clicking a link. Malware can come as an attachment with an email or as an embedded script.

Often, spam includes a link to a website that attempts to steal the user's money or download malware. For example, many websites advertise pharmaceutical drugs, but the websites never ship the drugs or the drugs that they ship are not authentic. Other times, a user can just click the link to a malicious website and become infected with a *driveby* download. A driveby

download automatically downloads and installs itself on the user's system without the user's knowledge.

Infected computers that have joined a botnet will often be directed to send out spam. If a computer is sending out spam without any user interaction, this is a clear indication that the system is infected and is a member of a botnet.

Phishing

The *phishing* email tries to trick users into providing their user name, password, or other personal information. It looks like it's from a legitimate source, but it's not. Attackers often send massive amounts of spam that include phishing attacks.

A phishing email often includes three elements. First, it lists a problem, such as suspicious activity on an account. Second, it includes a sense of urgency, such as a warning that your account will be locked out. Last, it includes a call to action, such as replying to an email with specific information or clicking a link and providing the information via a website.

For example, an attacker can send an email that looks like it's from PayPal or eBay, even using the same graphics as PayPal or eBay, but the email is completely fake. Another example is a notification that the user has won the lottery. To claim the winnings, the user needs to send back their address, phone number, and bank account number so that the winnings can be deposited into the account. Instead, the bank account is emptied.

NOTE **NEVER GIVE OUT YOUR PASSWORD**

Legitimate companies never request that their users validate passwords in an email. Any requests for sensitive information should be considered suspicious. An excellent basic security rule to follow is to never give out your password to anyone. When you start making exceptions, you can inadvertently give it out to a criminal. Another basic rule is to not click email links. If you want to check an account, type the address into the web browser so that you know you're going to the actual site.

Quick Check

1. **What type of malware requires a host?**
2. **What type of malware does not require a host?**

Quick Check Answers

1. **Virus.**
2. **Worm.**

Digital Security

Digital security refers to the technical methods used to protect systems. Antivirus and antispyware software are two primary digital security methods, but there are additional methods.

EXAM TIP

Security has become an important part of the A+ exams. The second domain of the 220-802 exam is titled "Security" and makes up 22 percent of the exam. This reflects the importance of security to organizations and how much they value security-conscious employees.

Antivirus Software

The best protection against malware is up-to-date antivirus (AV) software. *AV software* helps to prevent infections and to detect them when they occur.

AV software can detect multiple types of malware, not just viruses. For example, it's common for AV software to include the ability to detect viruses, worms, Trojan horses, adware, spyware, and other types of malware.

There are many AV software vendors. Some offer their products for free, and some companies sell their AV software. There's no requirement to get any specific version for any specific operating system.

However, you should consider it a security requirement to have some type of AV software running on every system you have. The only exception is a computer that never accesses the Internet, is not on a network, and never accepts files from external sources such as USB flash drives. A computer matching this description is rare, but if you have one, you might be able to do without AV software. Otherwise, you need it.

EXAM TIP

AV software should be installed and running on a computer before it connects to the Internet. Attackers are constantly scanning the Internet looking for unprotected systems.

AV Definitions and Updates

Malware has specific characteristics that AV software uses to identify the malware. For example, malware might be a specific size, have specific names, or have other characteristics that can identify them. These characteristics are stored in definition files used by the AV software.

AV software scans files and compares them against the definitions in the definition file. When a file has the same characteristics as a definition, the AV software identifies the malware and takes action to isolate it.

Definition files should be regularly updated. Criminals are constantly creating new malware and even different versions of old malware. If the definition file doesn't include the definition of a new virus, the AV software won't detect it. Years ago, IT professionals recommended updating the definitions once a week. Vendors now recommend updating them daily. Many AV programs will automatically check for updates several times a day and will download the updates when they're available.

EXAM TIP

You should check for updated definition files regularly. Many AV applications automatically check for updates one or more times a day. Also, it's common for AV software to include an option to automatically check for new definitions before running a scheduled scan.

Malware sometimes prevents a computer from receiving definition updates or system updates. If this is the case, you can often start the computer by using Safe Mode With Networking and retrieve the updates in this mode. You might also be able to download the definitions on another computer and copy them to the infected computer.

Antivirus Actions

When malware is detected, the AV software attempts to isolate it as quickly as possible, usually immediately. It suspends the activity of the malware and sends an alert to the user.

The alert can come in the form of a pop-up dialog box indicating the file is infected. Many Windows AV programs display a notification in the notification area that is on the far right of the taskbar. For example, Figure 26-2 shows an alert from Windows Defender.

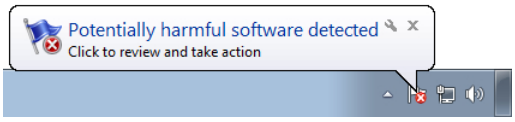


FIGURE 26-2 Windows Defender alert.

The alert usually provides a recommendation, such as blocking the activity, but the user can override the recommendation.

IMPORTANT **TAKE AV RECOMMENDATIONS SERIOUSLY**

Ignoring the recommendation can result in the malware running and infecting the user's system. Unless you're positive that the AV software is incorrect, you should not override the recommendation.

The two most common actions for AV software are as follows:

- **Quarantine.** A quarantined item is prevented from running and is often moved to a special location. Quarantined items can't cause damage to the system, but users can later restore the item if they determine that it is safe to do so.

- **Remove.** This deletes the item from the system. In some cases, the item can't be deleted immediately. Instead, the AV software quarantines it and the item is removed during the next restart cycle.

In many cases, the AV software allows the user to configure automatic actions. That is, instead of notifying the user of all activity, the AV software automatically takes the action.

For example, Figure 26-3 shows the settings for Microsoft Security Essentials. The default is normally "Recommended action" for each of these alerts. However, I changed the settings to show some of the different actions available.

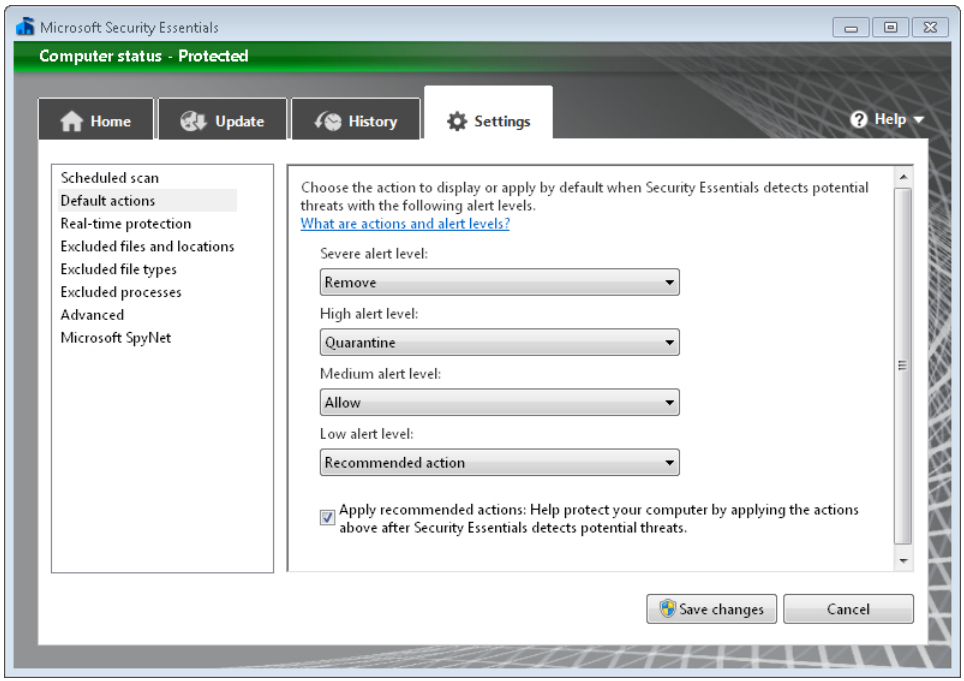


FIGURE 26-3 Microsoft Security Essentials settings on Windows 7.

Antivirus Protection

Most AV software provides protection on different levels, including the following:

- **Real-time protection.** The AV software constantly monitors any files that the user downloads or opens. For example, if a user downloads a file or opens a document, the AV software will scan it to determine whether it is malware. It also monitors system activity, looking for any suspicious actions.
- **Scheduled scans.** A scheduled scan runs at a specific time, such as every week at 1 AM on Sunday morning. It will start and run without user interaction. If the AV software doesn't include the ability to run a scheduled scan, you can sometimes schedule it with the Windows Task Scheduler.

- **On-demand scans.** If users or technicians suspect malicious activity is occurring, they can start a scan immediately to check the system.
- **Automatically update definitions.** This is usually built into the software. In some cases, the AV software will periodically check for updates, such as once or twice a day, and download updates only when there are changes. In other cases, the software checks based on a schedule, such as once a day.

Microsoft Security Essentials

Microsoft Security Essentials is free for home users and small businesses with up to 10 computers. It provides protection against many types of malware, including viruses, Trojan horses, worms, spyware, and more.

To get Microsoft Security Essentials, go to the Microsoft download site (*http://www.microsoft.com/download/*) and search on Windows Security Essentials. There are 32-bit and 64-bit versions. Make sure that you download the version that matches your CPU architecture.

In addition to providing real-time protection, Microsoft Security Essentials will also automatically check for updated definitions. During periods of high activity for new malware, it can update the definitions several times a day.

Figure 26-4 shows a screen shot of Microsoft Security Essentials in action after detecting a virus. You can click the Clean Computer button and it will take a recommended action based on the definition file. In most cases, it will remove the malware.

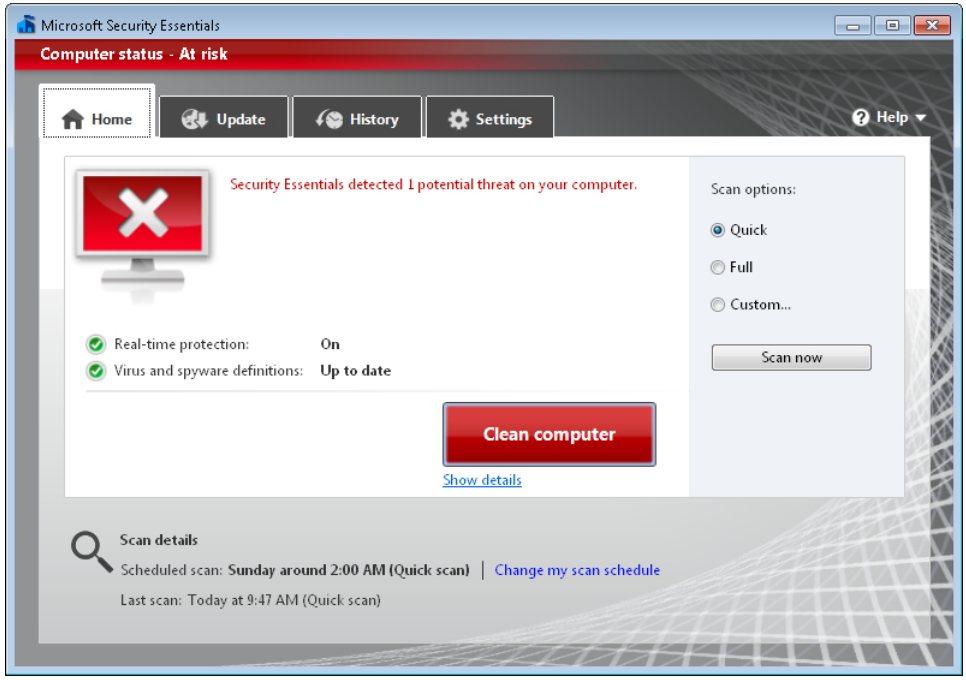


FIGURE 26-4 Microsoft Security Essentials alerting about malware.

Other AV Software

Just because Microsoft has free AV software available doesn't mean you have to use it. You might be running a non-Microsoft operating system, or you might choose to use AV software from another vendor. There are many reputable companies that offer AV software that you can purchase or download for free.

> ***IMPORTANT*** **WATCH OUT FOR ROGUEWARE**
>
> **The biggest warning related to free AV software is to beware of rogueware. Criminals have been known to post positive reviews of their rogueware on other sites. Therefore, just because someone posts a positive review on the Internet doesn't necessarily mean the software is valid. Trust your friends and reputable sources.**

Microsoft systems recognize many AV software applications, but not all of them. If you install AV software that is not recognized by Windows, it will show notifications indicating that the system is unprotected. However, you can let Windows know that you do have AV software installed and tell it to stop the notifications.

Figure 26-5 shows the Windows Action Center in Windows 7. If you've installed legitimate AV software but the Action Center indicates that your system doesn't have any AV software, you can click Turn Off Messages About Virus Protection. The display will change to Currently Not Monitored For Virus protection.

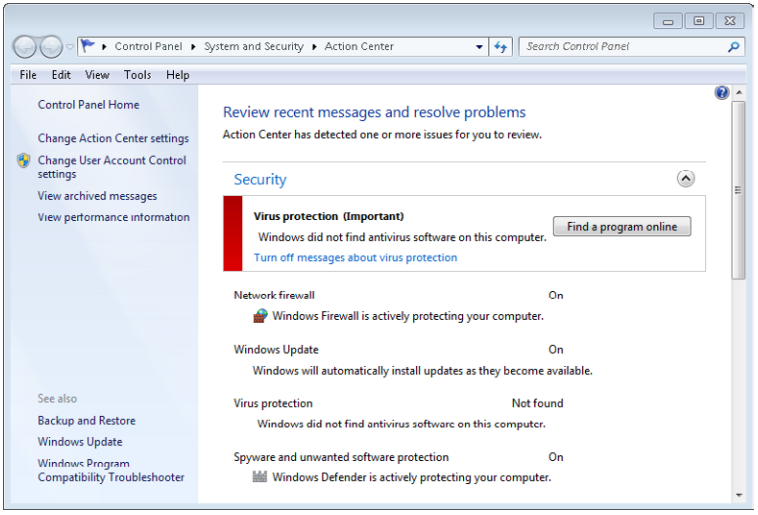


FIGURE 26-5 Microsoft Security Essentials Action Center.

NOTE **WINDOWS SECURITY CENTER NOW ACTION CENTER**

The Action Center was called the Windows Security Center in Windows XP and Windows Vista.

Automatically Starting AV Software

For AV software to be helpful, it needs to be running. Most AV software will automatically start when the system starts. However, malware sometimes changes these settings. You can use the System Configuration tool to verify that AV software is set to start automatically.

You can start the System Configuration tool by entering **msconfig** from the command prompt in any Windows-based system. Figure 26-6 shows this with the Startup tab selected. You can see that the Microsoft Security Client (which starts Microsoft Security Essentials) is deselected. A cool feature that's available with this is the Date Disabled column. You can use this to determine when it was disabled, and you might be able to connect it to the infection.

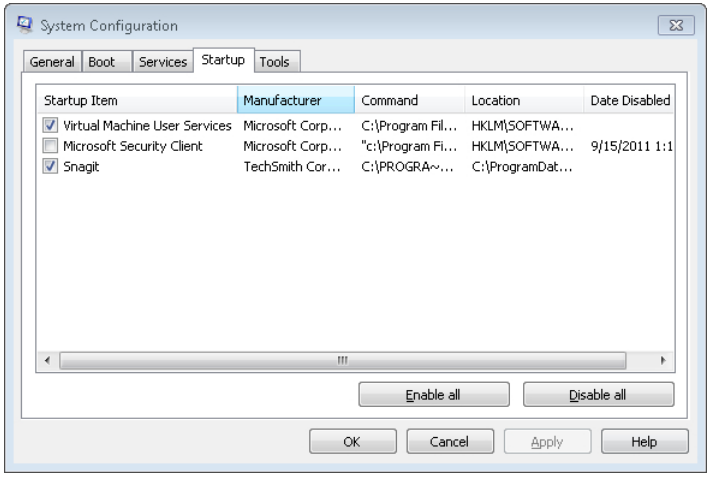


FIGURE 26-6 Verifying AV software set to start automatically.

In other cases, the service running the antivirus software might have been disabled. You can click the Services tab of the System Configuration utility and see whether any of the services are set to disabled. You can also view the running services from the Services applet available through the Control Panel.

Antispyware

Antispyware is software that is designed to look specifically for spyware. For example, Windows Defender is a free antispyware tool that is included with Windows Vista and Windows 7. It's also available as a free download for Windows XP. It attempts to prevent, remove, or quarantine spyware.

Many antivirus applications include antispyware capabilities. You can have separate antivirus and antispyware applications, but they can interfere with each other. Because of this, antivirus vendors often recommend that you do not run separate applications.

> ***TIP*** **WINDOWS SECURITY ESSENTIALS COVERS FOR WINDOWS DEFENDER**
>
> **If you are running Microsoft's Windows Security Essentials, Windows Defender won't run. Windows Security Essentials includes the capabilities of Windows Defender, so using both is unnecessary.**

Just as other AV software has definitions that need to be updated, Windows Defender uses updates. If you want to watch a short video showing how this is done, check out the following link: *http://windows.microsoft.com/en-us/windows7/keep-windows-defender-definitions-up-to-date*.

Keeping Systems Up to Date

Another protection against malware is keeping systems up to date. Malware often exploits vulnerabilities in operating systems. When these vulnerabilities are discovered, vendors release updates to eliminate the vulnerability.

For example, Microsoft releases patches and updates on the second Tuesday of every month (commonly called "Patch Tuesday"). Systems configured to apply updates automatically will download the updates and apply them without user action. It's also possible to configure a system to apply the updates manually.

Of course, these updates are useful only when they are applied. If the update is not applied, the system remains vulnerable. Malware authors love finding these systems, as the authors are often able to install malware onto a system without being detected.

Criminals are aware of the value of keeping a system up to date and have sometimes included code in malware to block updates. If you find that the Automatic Updates settings have changed or that you can't get updates, the system might be infected.

> ***MORE INFO*** **CHAPTER 15, "CONFIGURING WINDOWS OPERATING SYSTEMS"**
>
> **Chapter 15 covers Windows Update, how to enable Automatic Updates, and the importance of patch management practices used in organizations. If a system is not kept up to date against known security problems, it becomes an easy target.**

Disabling Autorun

The terms autorun and AutoPlay are often used interchangeably, but Microsoft makes a distinction between the two. A help article available in Windows 7, "What's the difference between AutoPlay and autorun?," defines the differences.

Autorun is a technology that automatically starts an application when media is inserted. For example, when you insert a CD, an application on the CD automatically starts. Autorun looks for a file named Autorun.inf, and if it is there, autorun reads it to identify which program to start. Autorun originally worked on any type of media, including optical discs, USB flash drives, and external hard drives.

MORE INFO **UPDATE INFORMATION ABOUT AUTORUN AND AUTOPLAY**

Microsoft Security Advisory 967940 (*http://technet.microsoft.com/security/advisory/967940*) discusses an update to autorun and AutoPlay. Specifically, it prevents AutoPlay from working with USB flash drives, external hard drives, or network shares on Windows XP and Windows Vista. This matches the functionality in Windows 7.

AutoPlay is a feature within Windows that allows you to define default actions. Instead of automatically starting the application defined in the Autorun.inf file, it gives the user additional choices.

While autorun was useful, criminals found ways to exploit it. They could add malware to the media and add or modify the Autorun.inf file. When the media was inserted into the system, autorun automatically installed the malware on the system. Before it was disabled on USB flash drives in Windows-based systems, malware was often spread from system to system with the help of autorun.

Here's a scenario that frequently occurs on unprotected systems. First, a single computer is infected. Among other tasks, the malware waits for a USB flash drive to be plugged in. When the flash drive is plugged in, the malware writes a virus file on the drive and also adds or modifies the Autorun.inf file to automatically start the virus when the drive is plugged into another system. When this USB flash drive is plugged into any other unprotected system, autorun installs the virus on the new system.

There are two primary ways that you can protect systems. First, ensure that all systems have up-to-date antivirus software running. Second, ensure that AutoPlay is not configured to automatically run applications from USB drives or from any other media.

On Windows XP, you can access AutoPlay settings from Windows Explorer. Right-click an optical disc drive, select Properties, and click the AutoPlay tab.

On Windows Vista and Windows 7, you can access the AutoPlay applet in Control Panel from a list view.

Figure 26-7 shows a typical pop-up (on the left) that appears when you insert an optical disc in a drive. This disc came with an HP printer. I can click Run Setup.exe and it will run the install program. It's possible to select Always Do This For Software And Games, although it isn't recommended. If you ever want to change the settings, you can start AutoPlay (shown on the right).

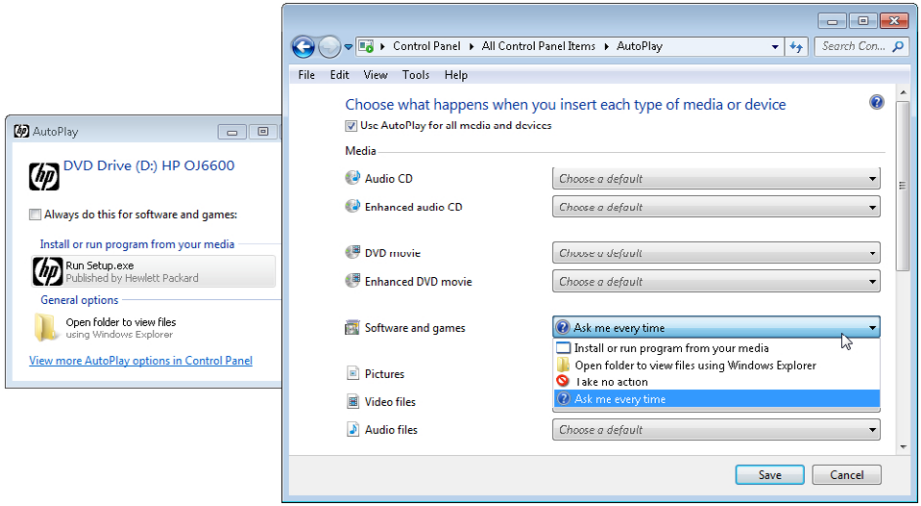


FIGURE 26-7 Viewing AutoPlay settings.

EXAM TIP

As a security best practice, autorun should be disabled. Any setting except Install or Run Program From Your Media will prevent an application from automatically starting.

Each of the settings includes a drop-down box, and for security reasons, the default setting for Software And Games is Ask Me Every Time. This prevents potentially malicious software from running automatically. If you want to completely disable it, select Take No Action.

Figure 26-7 shows the Use AutoPlay For All Media And Devices setting selected. This does not include USB flash drives or hard drives. It does include devices such as cameras, tablets, and MP3 players.

Quick Check

1. **How often should AV definitions be updated?**
2. **What tools can you use to verify that your antivirus software is set to start automatically?**

Quick Check Answers

1. **Regularly, such as once a day, but not less than once a week.**
2. **System Configuration (msconfig) and Services.**

Symptoms of an Infection

When a computer is infected with malware, the system will give you a variety of different indications. The following list describes many of the common symptoms of an infection:

- **Security alerts.** One of the primary symptoms is a report from antivirus or antispyware software of the infection. It's common for antivirus software to show a pop-up window indicating that the system is infected. You might also see errors in the Event Viewer (covered in Chapter 17, "Troubleshooting Windows Operating Systems").
- **Random pop-up advertisements.** The malware is often trying to get you to click a link which will likely take you to a malicious web site.
- **Slow performance.** Malware activity can often consume system resources. It can cause random disk or network activity and consume processor and memory.

EXAM TIP

Unusual disk activity could be from a virus spreading on your computer, but it could also be due to other issues. It might be that AV software is scanning your system, your disk is fragmented and needs to be defragmented, or you don't have enough RAM and your system has excessive paging.

- **Spontaneous shutdown/restart.** When the malware interferes with the operating system, it can cause the system to restart itself. At other times, it can stop and show a stop error.
- **PC locks up.** Instead of restarting, the system might just stop responding to keyboard or mouse input.
- **Won't perform familiar tasks.** For example, an application might stop running or no longer start. In some cases, a user might no longer be able to access a familiar website.
- **Changes to files.** Malware can rename system files, delete files, or modify permissions without user interaction. If a user is authorized to access a file or folder but sees an Access Denied message when accessing it, it can be an indication that malware has modified the permissions.
- **Can't access hardware.** In some cases, the malware will interfere with accessing some disk drives, printers, or other hardware.
- **Windows Update failures.** Malware sometimes modifies the system configuration settings to prevent updates.
- **Browser redirection.** When you try to access a known site, the system takes you to a different website.
- **Browser modifications.** Some malware resets the home page, modifies the proxy settings, and/or installs unauthorized add-ins.

- **Internet connectivity issues.** Often, malware will modify the web browser proxy server settings. Instead of accessing the Internet through the proxy server, the system tries to access the Internet through other paths. This can bypass security protections from the proxy server, or it might block Internet access for the system until the settings are restored.
- **Antivirus software disabled.** Malware often tries to disable antivirus software so that the malware can run unimpeded.
- **Access denied or other unusual error messages.** Error messages might be from the operating system reporting errors. They might also be from the malware itself trying to trick the user into clicking a link. If malware is trying to install software on its own, User Account Control (UAC) will block it with an Access Denied error.

EXAM TIP

When you clean an instance of malware on a system, it will often try to reinstall itself from a temporary location. Windows 7 includes checks to block this. It might give an Access Denied error with a title of RunDLL. In other cases, UAC might prompt you to approve an installation even though you aren't installing anything.

- **Unusual network activity.** Some malware tries to infect other systems over the network. If the computer has joined a botnet, it will check in with the botnet herder for instructions and might start attacks on others.
- **Files with double extensions.** File extensions like .txt.exe or .jpg.exe are not normal. Malware sometimes overwrites existing files and just adds the extra extension. For example, Figure 26-8 shows Windows Explorer without extensions on the left and with extensions on the right. The Sunrise.JPG.vbs file is a malicious Visual Basic script. A user might be fooled into thinking that the .vbs file is a .jpg file. If a .vbs file is double-clicked, the malicious script will run.

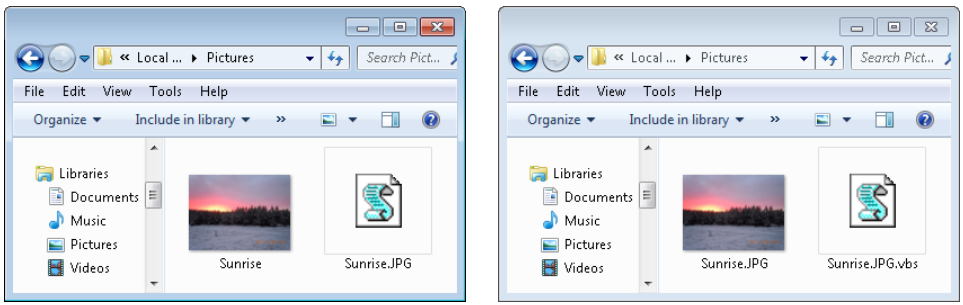


FIGURE 26-8 Viewing files with and without extensions.

MORE INFO **CHAPTER 13, "USING WINDOWS OPERATING SYSTEMS"**

You can modify how extensions are viewed by using the Folder Options applet in Control Panel. Chapter 13 includes steps for modifying these settings.

This is certainly not an all-inclusive list. The key to recognizing malware is recognizing unusual or suspicious activity. If you detect anything out of the ordinary, it's worth your time to update the definitions and run a virus scan.

Removing Malware

Antivirus software is often unable to remove a virus, so you need to remove it manually. When this is the case, antivirus software vendors often have step-by-step instructions for how to remove all elements of the virus.

Some organizations have a policy of completely reimaging a computer after an infection rather than trying to clean it. In some extreme cases, you also need to completely reformat the disk and reinstall the operating system. However, there are other steps you can take to clean and remove some malware.

EXAM TIP

Criminals often write very sophisticated malware, but there are many talented professionals that dissect it to learn how it works and how to remove it. When standard steps for removing malware aren't effective, the best source for additional information is antivirus websites. Microsoft also maintains some sites with valuable security information. For example, the Malware Protection Center (*http://www.microsoft.com/Security/portal/*) includes timely information on current threats.

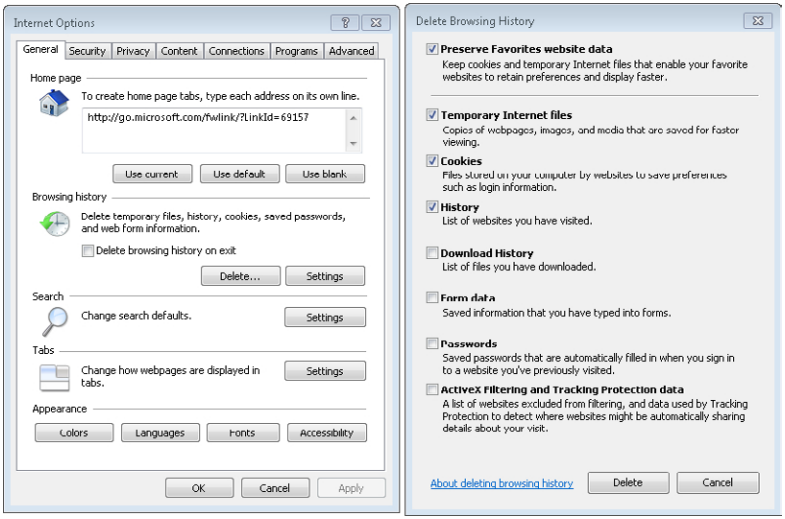
Delete Temporary Files

Malicious software often hides itself within temporary files stored on your hard drive. Malware often stores a copy of itself there, and if the original is discovered and deleted, it later restores itself.

You can delete these files by using the web browser settings. For example, if you're running Internet Explorer 9, you can use the following steps:

1. Start Internet Explorer.
2. Click Tools, and select Internet Options.
3. Ensure that the General tab is selected. Click the Delete button.

4. On the Delete Browsing History page, ensure that Temporary Internet Files is selected, as shown in the following graphic. Click Delete. When the file deletion completes, click OK.



You can also use the Disk Cleanup tool in Windows-based systems to delete temporary files. The following steps show how:

1. Start Windows Explorer.
2. Right-click the C drive and select Properties.
3. Click Disk Cleanup.
4. Ensure that Temporary Internet Files is selected. You might also want to select the Temporary Files selection, but you'll have to scroll down to see it.
5. Click OK. A pop-up window will ask whether you're sure you want to permanently delete the files. Click Delete Files.
6. After a moment, the Disk Cleanup page will appear. Click OK.

Using Safe Mode

Safe Mode can be very useful when removing malware. Sometimes the antivirus software can't remove the software normally, but when you run it in Safe Mode, it can remove the malware. Other times you might need to delete a file, but you'll be able to do so only from Safe Mode.

EXAM TIP

If the system prevents you from deleting a file and reports that the file is in use, you can usually delete the file from Safe Mode. There are other tools that you can also use. For example, you might be able to use the del (delete) command with the /f switch to delete a file, or you might use a third-party tool.

Because Safe Mode starts with a minimal set of drivers and services, the malware usually won't be started and can't protect itself. Chapter 17 talks about Safe Mode in greater depth, but in brief, you can access Safe Mode on Windows-based systems with the following steps:

1. Reboot your system.
2. Press F8 as the computer starts but before the Windows logo appears. This will give you access to the Advanced Options menu.
3. Select Safe Mode.

EXAM TIP

If you need to update definitions for your AV software, you'll need to select Safe Mode With Networking.

Using Preinstallation Environments

In some cases, Safe Mode can't detect or remove all malicious software, and you might need to use a preinstallation environment (PE). Windows PE is used during the installation of Windows and during some Windows recovery operations. For example, if you run Windows memory diagnostics, it runs in a Windows Recovery Environment, which is an enhanced Windows PE.

A preinstallation environment with antivirus tools is often referred to as an offline scanning kit. Microsoft has published the Infrastructure Planning and Design Malware Response document, and Appendix C of that document includes steps that you can use to create an offline scanning kit. This document also includes detailed steps and flow charts that you can use to troubleshoot an infected computer. You can access the download here: *http://go.microsoft.com/fwlink/?LinkId=93108*.

EXAM TIP

You can boot into any alternate operating system and then run antivirus software to remove malware. This is often effective when removing malware that is embedded in the boot sector or the master boot record. Alternate operating systems can be a preinstallation environment, a basic operating system on a 3.5-inch floppy drive, or an operating system booted from a CD or DVD.

If you already have an alternate operating system, a good tool to have is Microsoft's Malicious Software Removal Tool. You can get a free copy from Microsoft. The following page provides more information about the tool, including a link to download it: *http://www.microsoft.com/security/pc-security/malware-removal.aspx*.

Using Recovery Console and Windows RE

In some cases, you might need to use the Recovery Console on Windows XP or the Windows Recovery Environment (Windows RE) on Windows Vista or Windows 7. This is especially useful if the malware has modified the disk.

You can use commands such as fixboot to repair an infected boot sector or fixmbr to repair a damaged master boot record (mbr) from the Recovery Console. Similarly, you can use the bootrec /fixboot and bootrec /fixmbr commands from the Windows RE.

> ***MORE INFO*** **CHAPTER 17**
>
> **Chapter 17 covers many troubleshooting tools, including the Recovery Console and the Windows RE.**

System Restore

In some cases, you can remove malware by restoring your system to a previous state with System Restore. Use the procedures described in Chapter 15 to use System Restore.

Best Practices for Malware Removal

There are several steps you can take that are considered best practices for malware removal on Windows systems. The following steps outline these practices:

1. **Identify malware symptoms.** The list in the "Symptoms of an Infection" section earlier in this chapter identifies common symptoms.
2. **Quarantine infected system.** You quarantine a system by isolating it from other systems. Most computers are on networks today, and if you can disconnect a computer from the network, you have quarantined it. This is as simple as unplugging the network cable.

EXAM TIP

When removing malware, it's often useful to isolate the system by removing its Internet access. You can do this by removing the network cable to the computer or by disabling the network interface card.

3. **Disable system restore.** While removing malware, you will likely make modifications that would normally be captured by system restore. By disabling system restore, you ensure that a user can't accidentally reinfect the system by applying a restore point.
4. **Remediate infected system.** Ensure that the antivirus software is up to date. If necessary, you might need to copy definition files from an uninfected system, but you do not want to connect the infected system to the network or to the Internet. Next, use tools to scan and remove the malware. You might need to use Safe Mode or a preinstallation environment.
5. **Schedule scans and updates.** After cleaning the system, ensure that the antivirus software is configured to regularly retrieve updates and scan the system for malware.
6. **Enable system restore and create restore point.** This normalizes the system and provides a known clean restore point. If the system develops a different problem later, you can use this restore point. If you use an earlier restore point, it's possible that you will re-infect the system again.
7. **Educate end user.** End users often do not understand the risks related to computers and can easily fall prey to common criminal tactics. You can help prevent a reoccurrence of many problems and also help end users avoid suffering from personal losses with just a little education. Users aren't always as receptive to this information prior to an incident, but they become very interested after one.

Quick Check

1. Name two ways you can delete temporary files.
2. What mode can you use if antivirus software can't clean malware when started normally?

Quick Check Answers

1. By using Disk Cleanup and through the web browser options.
2. Safe Mode or Safe Mode with Networking.

Recognizing Other Security Threats

The first part of this chapter covers malware, but there are some other common security threats that you should know about. Most organizations have become much more security-conscious, and they realize that one of the best prevention tactics against threats is to have knowledgeable employees.

Employees who understand these threats are less likely to be tricked by them. Additionally, these employees are more likely to support the policies designed to thwart attackers and criminals.

Social Engineering

Social engineering is a fancy way of saying that attackers or criminals attempt to fool people by using social methods. The attacker uses trickery and conniving to get people to do something they wouldn't normally do.

For example, if a stranger asks you to give him your password, you probably wouldn't. On the other hand, imagine the following scenario.

An employee named Sally receives a phone call from someone identifying himself as an IT professional within the company. He tells Sally that her system is infected with a virus that will destroy all her data and that she needs to turn her computer off. Someone from IT will be around to fix her computer within a week.

Instead of doing without a computer for a week, Sally says, "Wait. I need my computer. Isn't there another way this can be fixed?"

The IT professional (who is actually a criminal impersonating an IT professional) says, "Well, I can fix your system over the network. I have to use your account and password. Don't tell anyone I'm doing this for you because everyone will want me to do it for them too." Sally then gladly gives this social engineer her user name and password.

This is just one example of social engineering, but criminals use many more. Some examples of social engineering tactics are as follows:

- If a stranger asks you to give him money for bogus software or to install a virus in your system, you probably wouldn't. Yet rogueware tricks people into taking both of these actions.
- Most people wouldn't give a stranger their user names and passwords for bank accounts. However, carefully worded phishing emails and sophisticated lookalike websites regularly trick people into giving up this information.
- Criminals impersonating bank employees have called people to verify account information. What they're actually doing is collecting account information so that they can empty the account.
- Employees wouldn't normally allow strangers into internal company locations. However, a criminal impersonating a phone company employee or pest control technician might be granted free and unsupervised access.

Some criminals use a social engineering attack as part of a more sophisticated point. For example, a criminal might call and trick employees into giving up information about executives. The criminal can then launch a *whaling attack*, which is a phishing attack targeted at executives.

Physical Security

Physical security includes securing anything you can touch, such as by locking doors or shredding documents. There are some specific threats related to security that PC technicians should understand, along with basic methods of preventing problems.

Tailgating

Many organizations control access to workspaces by using electronic badges or cipher locks. They swipe their badge across a reader and it opens the door, or they enter the code in the cipher lock to open the door. The locked door keeps unauthorized people out, but attackers can bypass it with a simple practice known as *tailgating*.

An attacker can follow closely behind an employee, and when the employee opens the door, the attacker simply follows behind. The attacker doesn't need a badge or the cipher code. If an attacker is wearing a bad-guy mask, employees are less likely to allow this practice. However, instead of a mask, attackers often have a friendly, disarming smile.

Educating employees about tailgating helps stop it. Another method is to have turnstiles that allow only one person to pass through at a time.

Securing or Shredding Physical Documents

Printed documents can include a great wealth of data, and if left unsecured, the information can easily be stolen. Many organizations implement a clean desk policy that requires employees to secure physical documents. They might lock the documents in a drawer or safe, but the documents aren't left where anyone can see them. Similarly, passwords should never be written down and left in plain sight.

Dumpster diving is the practice of looking through trash to find information. People often throw away papers that have valuable information, and a criminal can just look through the trash to get the data. A simple way of preventing criminals' success is by shredding documents instead of throwing them away. Many home users have recognized the importance of this and have home shredders.

Shoulder Surfing and Privacy Filters

Shoulder surfing is the practice of looking over someone's shoulders to view what they're typing on the screen or to watch what they type on the keyboard.

For example, employees might process sensitive data on their computer. The data is protected from unauthorized access with permissions, but if criminals can just look over someone's shoulders and get the information, they don't have to take the time and effort to hack into a system.

A simple protection against shoulder surfing is the use of privacy filters. They limit the viewing angle of the monitor and can reduce the success of shoulder surfers.

> ***MORE INFO*** **CHAPTER 6, "EXPLORING VIDEO AND DISPLAY DEVICES"**
>
> **Privacy and antiglare filters are mentioned in Chapter 6. They can be used to reduce eyestrain and to increase security.**

Chapter Summary

- Malicious software (malware) is software written by malicious users with the intent to cause harm or damage.
- Criminals run botnets, which are groups of infected computers acting as zombies. These zombies do whatever they're commanded to do.
- Different types of malware have different behaviors and intended outcomes.
  - A virus requires a host file. When the host file executes, the malicious code in the virus executes.
  - A worm does not require a host file. It self-replicates over a network without user interaction.
  - A Trojan appears to be one thing but is something else.
  - Rogueware is fake antivirus software offered for free but used to collect money from unsuspecting users.
  - Rootkits take over the system from users and antivirus software.
  - Spyware installs itself on a user's system or modifies a user's system without the user's knowledge or consent.
  - Spam is unwanted email. Malware is often spread through the Internet as email attachments.
  - Phishing is malicious email sent to a large group of people trying to trick them. It often tries to get the user to give up personal information such as a user name and password.
- Antivirus software is the best protection against malware. Most AV software protects against multiple types of malware, not just viruses.
- AV software identifies viruses by using definitions. Definitions should be updated regularly, such as once a day.
- AV software will try to remove or quarantine malware. Quarantined files can be retrieved if desired.
- Most AV software will start automatically when the system starts, but malware sometimes tries to change this behavior. You can use msconfig to verify that the AV software starts automatically.
- Systems should be kept up to date to avoid infections. This includes keeping antivirus software up to date with current definitions and keeping the operating system up to date.
- Any type of unusual activity can indicate an infection. Run AV software to verify that the system is not infected.
- Deleting temporary files can often remove malware remnants on a system and prevent reinfections.

- Safe Mode is useful for removing malware that can be removed normally. If you need to download up-to-date definitions, use Safe Mode With Networking.
- Social engineers attempt to trick users into giving up information or taking actions that they wouldn't normally take.
- Physical security methods help prevent attacks such as tailgating, dumpster diving, and shoulder surfing.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the "Answers" section at the end of this chapter.

1. Which of the following can spread without user interaction?
   - **A.** Virus
   - **B.** Worm
   - **C.** Trojan horse
   - **D.** Botnet
2. After installing a free game, a user's system began acting erratically. It showed unusual errors and was randomly rebooting. What does this describe?
   - **A.** Worm
   - **B.** Rogueware
   - **C.** Trojan horse
   - **D.** Spam
3. Lori received an email that indicates it's from her bank, saying there is a problem with her account. The email asks her to verify her account information. What best describes this?
   - **A.** Trojan horse
   - **B.** Spyware
   - **C.** Adware
   - **D.** Phishing email

4. A user hasn't connected to the Internet in several weeks. The user was recently infected with a virus from a USB even though the user has AV software installed. What should be done?

   A. Purchase newer AV software.

   B. Reinstall the operating system.

   C. Update the AV software definitions.

   D. Enable the Windows Firewall.

5. A user has AV software installed, and the software previously ran all the time. However, it no longer starts automatically. What's the likely reason?

   A. The software has been removed.

   B. The service is set to disabled.

   C. It's configured to start only in Safe Mode.

   D. Windows Defender is running.

6. A user's system is infected with a virus, and the virus is preventing the AV software from obtaining up-to-date definitions for installed AV software. What should be done? (Choose all that apply.)

   A. Start in Safe Mode and download the definitions.

   B. Start in Safe Mode With Networking and download the definitions.

   C. Download the definitions on another computer and copy them to the infected computer.

   D. Use System Restore to return your system to a previous state.

7. You have discovered a malicious file on your computer. When you try to delete it, the system reports that the file is in use and prevents the deletion. What should you do?

   A. Start the Action Center and delete it from there.

   B. Delete the file from the command prompt.

   C. Boot into BIOS and disable password protection.

   D. Boot into Safe Mode and then delete the file.

Answers

This section contains the answers to the chapter review questions in this chapter.

1. **Correct Answer:** B
   - **A. Incorrect:** A virus attaches itself to an application and requires user interaction to spread.
   - **B. Correct:** A worm is self-replicating and will spread without user interaction.
   - **C. Incorrect:** A Trojan horse is a type of malware that appears to be one thing but also includes something else that is malicious.
   - **D. Incorrect:** Computers can join a botnet after becoming infected with a virus, but the botnet itself doesn't spread.
2. **Correct Answer:** C
   - **A. Incorrect:** A worm is self-replicating, so it is not installed with a game.
   - **B. Incorrect:** Rogueware is fake AV software.
   - **C. Correct:** A Trojan horse looks like one thing (such as a free game) but also installs something malicious.
   - **D. Incorrect:** Spam is unwanted email.
3. **Correct Answer:** D
   - **A. Incorrect:** The user might be tricked into installing a Trojan horse after clicking a link in a phishing email, but the email itself is not a Trojan horse.
   - **B. Incorrect:** Spyware will try to collect information about users, but this can't be done just from the email.
   - **C. Incorrect:** Adware pops up advertisements, but it does not send email to users.
   - **D. Correct:** A phishing email purports to come from a legitimate company and tries to trick the user into giving up personal information. Legitimate companies do not ask users to verify account information in this way.
4. **Correct Answer:** C
   - **A. Incorrect:** The existing AV software might be adequate if it has up-to-date definitions.
   - **B. Incorrect:** It is not necessary to reinstall the operating system.
   - **C. Correct:** If the computer hasn't connected to the Internet in several weeks, the virus definitions are out of date and should be updated.
   - **D. Incorrect:** The Windows Firewall won't block viruses.

5. **Correct Answer:** B

   A. **Incorrect:** The scenario says it is installed.

   B. **Correct:** One way that malware protects itself is by disabling the service for AV software. If the service previously started automatically, this should be checked.

   C. **Incorrect:** Applications are not configured to start only in Safe Mode.

   D. **Incorrect:** Windows Defender does not prevent AV software from running.

6. **Correct Answer:** B, C

   A. **Incorrect:** Safe Mode without networking won't provide access to the Internet.

   B. **Correct:** Starting Safe Mode With Network will allow you to connect to the Internet to download the definitions.

   C. **Correct:** Updating definitions on another computer and then copying them to the infected computer will work.

   D. **Incorrect:** System Restore repairs many problems, but it does not update malware definitions.

7. **Correct Answer:** D

   A. **Incorrect:** The Action Center reports on current security settings, but it doesn't include the ability to delete files.

   B. **Incorrect:** If the file is protected because it's in use, you won't be able to delete it from the command prompt.

   C. **Incorrect:** BIOS password protection can protect the BIOS, but it doesn't affect how files are protected when the system is booted.

   D. **Correct:** Safe Mode uses minimal drivers and services. You can often delete files in Safe Mode that you can't delete normally.