Objectives

After completing this chapter, you will be able to:

1. Define the term, computer security risks, and briefly describe the types of cybercrime perpetrators: hacker, cracker, script kiddie, corporate spy, unethical employee, cyberextortionist, and cyberterrorist.

2. Describe various types of Internet and network attacks (computer viruses, worms, Trojan horses, rootkits, botnets, denial of service attacks, backdoors, and spoofing), and identify ways to safeguard against these attacks, including firewalls, intrusion detection software, and honeypots.

3. Discuss techniques to prevent unauthorized computer access and use.

4. Identify safeguards against hardware theft and vandalism.

5. Explain the ways software manufacturers protect against software piracy.

6. Discuss how encryption works, and explain why it is necessary.

7. Discuss the types of devices available that protect computers from system failure.

8. Explain the options available for backing up computer resources.

9. Identify risks and safeguards associated with wireless communications.

10. Discuss ways to prevent health-related disorders and injuries due to computer use.

11. Recognize issues related to information accuracy, intellectual property rights, codes of conduct, and green computing.

12. Discuss issues surrounding information privacy, including electronic profiles, cookies, spyware and adware, spam, phishing, privacy laws, social engineering, employee monitoring, and content filtering.
Computer Security Risks

Today, people rely on computers to create, store, and manage critical information. Thus, it is important that computers and the data they store are accessible and available when needed. It also is crucial that users take measures to protect their computers and data from loss, damage, and misuse. For example, organizations must ensure that sensitive data and information such as credit records, employee and customer data, and purchase information is secure. Home users must ensure that their credit card number is secure when they use it for online purchases.

A computer security risk is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability. While some breaches to computer security are accidental, many are intentional. Some intruders do no damage; they merely access data, information, or programs on the computer before logging off. Other intruders indicate some evidence of their presence either by leaving a message or by deliberately altering or damaging data.

An intentional breach of computer security often involves a deliberate act that is against the law. Any illegal act involving a computer generally is referred to as a computer crime. The term cybercrime refers to online or Internet-based illegal acts. Software used by cybercriminals sometimes is called crimeware. Today, cybercrime is one of the FBI's top three priorities.

Perpetrators of cybercrime and other intrusions fall into seven basic categories: hacker, cracker, script kiddie, corporate spy, unethical employee, cyberextortionist, and cyberterrorist.

- The term hacker, although originally a complimentary word for a computer enthusiast, now has a derogatory meaning and refers to someone who accesses a computer or network illegally. Some hackers claim the intent of their security breaches is to improve security.
- A cracker also is someone who accesses a computer or network illegally but has the intent of destroying data, stealing information, or other malicious action. Both hackers and crackers have advanced computer and network skills.
- A script kiddie has the same intent as a cracker but does not have the technical skills and knowledge. Script kiddies often use prewritten hacking and cracking programs to break into computers.
- Some corporate spies have excellent computer and networking skills and are hired to break into a specific computer and steal its proprietary data and information, or to help identify security risks in their own organization. Unscrupulous companies hire corporate spies, a practice known as corporate espionage, to gain a competitive advantage.
- Unethical employees may break into their employers’ computers for a variety of reasons. Some simply want to exploit a security weakness. Others seek financial gains from selling confidential information. Disgruntled employees may want revenge.
• A **cyberextortionist** is someone who uses e-mail as a vehicle for extortion. These perpetrators send an organization a threatening e-mail message indicating they will expose confidential information, exploit a security flaw, or launch an attack that will compromise the organization’s network — if they are not paid a sum of money.

• A **cyberterrorist** is someone who uses the Internet or network to destroy or damage computers for political reasons. The cyberterrorist might target the nation’s air traffic control system, electricity-generating companies, or a telecommunications infrastructure. The term, **cyberwarfare**, describes an attack whose goal ranges from disabling a government’s computer network to crippling a country. Cyberterrorism and cyberwarfare usually require a team of highly skilled individuals, millions of dollars, and several years of planning.

Business and home users must protect, or safeguard, their computers from breaches of security and other computer security risks. Some organizations hire individuals previously convicted of computer crimes to help identify security risks and implement safeguards because these individuals know how criminals attempt to breach security.

The more common computer security risks include Internet and network attacks, unauthorized access and use, hardware theft, software theft, information theft, and system failure (Figure 11-1). The following pages describe these computer security risks and also discuss safeguards users might take to minimize or prevent their consequences.

**Figure 11-1** Computers and computer users are exposed to several types of security risks.
Internet and Network Attacks

Information transmitted over networks has a higher degree of security risk than information kept on an organization’s premises. In an organization, network administrators usually take measures to protect a network from security risks. On the Internet, where no central administrator is present, the security risk is greater.

To determine if your computer is vulnerable to an Internet or network attack, you could use an online security service. An online security service is a Web site that evaluates your computer to check for Internet and e-mail vulnerabilities (Figure 11-2). The service then provides recommendations of how to address the vulnerabilities.

Companies and individuals requiring assistance or information about Internet security breaches can contact or visit the Web site for the Computer Emergency Response Team Coordination Center, or CERT/CC, which is a federally funded Internet security research and development center.

Internet and network attacks that jeopardize security include computer viruses, worms, Trojan horses, and rootkits; botnets; denial of service attacks; back doors; and spoofing. The following pages address these computer security risks and suggest measures organizations and individuals can take to protect their computers while on the Internet or connected to a network.

A computer virus is a potentially damaging computer program that affects, or infects, a computer negatively by altering the way the computer works without the user’s knowledge or permission. Once the virus infects the computer, it can spread throughout and may damage files and system software, including the operating system.

A worm is a program that copies itself repeatedly, for example in memory or on a network, using up resources and possibly shutting down the computer or network.

A Trojan horse (named after the Greek myth) is a program that hides within or looks like a legitimate program. A certain condition or action usually triggers the Trojan horse. Unlike a virus or worm, a Trojan horse does not replicate itself to other computers.

A rootkit is a program that hides in a computer and allows someone from a remote location to take full control of the computer. Once the rootkit is installed, the rootkit author can execute programs, change settings, monitor activity, and access files on the remote computer. Although rootkits can have legitimate uses, such as in law enforcement, their use in nefarious and illegal activities is growing rapidly.

Computer viruses, worms, Trojan horses, and rootkits are classified as malware (short for malicious software), which are programs that act without a user’s knowledge and deliberately alter the computer’s operations. Other classes of malware include back doors and spyware, which are discussed later in this chapter. Although malware often falls in one of these classes (virus, worm, Trojan horse, rootkit, back door, or spyware), some malware has characteristics of two or more classes. For example, MyDoom and Blaster are worms; Melissa has elements of a virus, worm, and Trojan horse.

Unscrupulous programmers write malware and then test it to ensure it can deliver its payload. The payload is the destructive event or prank the program is intended to deliver.

A computer infected by a virus, worm, Trojan horse, or rootkit often has one or more of the following symptoms:

- Operating system runs much slower than usual
- Available memory is less than expected
- Files become corrupted
- Screen displays unusual message or image
- Music or unusual sound plays randomly

Computer Viruses, Worms, Trojan Horses, and Rootkits

Every unprotected computer is susceptible to the first type of computer security risk — a computer virus, worm, Trojan horse, and/or rootkit.

<table>
<thead>
<tr>
<th>Name of Online Service</th>
<th>Web Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee FreeScan</td>
<td><a href="http://home.mcafee.com/Downloads/FreeScan.aspx">http://home.mcafee.com/Downloads/FreeScan.aspx</a></td>
</tr>
<tr>
<td>Trend Micro House Call</td>
<td><a href="http://housecall.trendmicro.com/">http://housecall.trendmicro.com/</a></td>
</tr>
</tbody>
</table>

Figure 11-2 Some popular online security services.
How a Virus Can Spread through an E-Mail Message

Step 1
Unscrupulous programmers create a virus program that deletes all files. They hide the virus in a word processing document and attach the document to an e-mail message.

Step 2
They send the e-mail message to thousands of users around the world.

Step 3a
Some users open the attachment and their computers become infected with the virus.

Step 3b
Other users do not recognize the name of the sender of the e-mail message. These users do not open the e-mail message — instead, they immediately delete the e-mail message and continue using their computers. These users’ computers are not infected with the virus.

Malware delivers its payload on a computer in a variety of ways: when a user (1) opens an infected file, (2) runs an infected program, (3) boots the computer with infected removable media inserted in a drive or plugged in a port, (4) connects an unprotected computer to a network, or (5) when a certain condition or event occurs, such as the computer’s clock changing to a specific date. Today, a common way computers become infected with viruses and other malware is through users opening infected e-mail attachments (Figure 11-3).

Currently, more than 300,000 Web sites can infect your computer with known viruses, worms, Trojan horses, rootkits, and other malware. Many Web sites maintain lists of all known malware. For a more technical discussion about these types of malware, read the High-Tech Talk article on page 178 in Chapter 3.

Can multimedia files be infected with a virus?
Yes. The increase in popularity of media sharing Web sites provides a great opportunity to distribute malicious programs. During one year, approximately 500,000 people downloaded what they thought was a media file from the Internet. In fact, the file was a Trojan horse that infected many computers with spyware. For this reason, it is important to scan all media files for malware before playing them.

FAQ 11-1
For more information, visit scsite.com/dc2011/ch11/faq and then click Infected Media Files.

Figure 11-3 This figure shows how a virus can spread through an e-mail message.
Some viruses are hidden in macros, which are instructions saved in software such as a word processing or spreadsheet program. In programs that allow users to write macros, you should set the macro security level so that the application software warns users that a document they are attempting to open contains a macro (Figure 11-4). From this warning, a user chooses to disable or enable the macro. If the document is from a trusted source, the user can enable the macro. Otherwise, it should be disabled.

Users should install an antivirus program and update it frequently. As Chapter 8 discussed, an antivirus program protects a computer against viruses by identifying and removing any computer viruses found in memory, on storage media, or on incoming files. Most antivirus programs also protect against other malware. When you purchase a new computer, it often includes antivirus software. Many e-mail servers also have antivirus programs installed to check incoming and outgoing e-mail messages for malware. The table in Figure 11-5 lists popular antivirus programs.

An antivirus program scans for programs that attempt to modify the boot program, the operating system, and other programs that normally are read from but not modified. In addition, many antivirus programs automatically scan files downloaded from the Web, e-mail attachments, opened files, and all types of removable media inserted in the computer.

One technique that antivirus programs use to identify a virus is to look for virus signatures. A virus signature, also called a virus definition, is a known specific pattern of virus code. Computer users should update their antivirus program’s signature files regularly (Figure 11-6). This

---

**Safeguards against Computer Viruses and Other Malware**

Methods that guarantee a computer or network is safe from computer viruses and other malware simply do not exist. Users can take several precautions, however, to protect their home and work computers and mobile devices from these malicious infections. The following paragraphs discuss these precautionary measures.

Do not start a computer with removable media inserted in the drives or plugged in the ports. For example, optical disc drives should be empty, and a USB port should not contain a USB flash drive. During the startup process, a computer may attempt to execute the boot sector on media in certain drives and ports. Even if the attempt is unsuccessful, a virus on the boot sector of removable media can infect the computer’s hard disk. If you must start the computer with media in a drive or port, be certain the media are uninfected or from a trusted source. A trusted source is an organization or person you believe will not send a virus infected file knowingly.

Never open an e-mail attachment unless you are expecting the attachment and it is from a trusted source. If the e-mail message is from an unknown source or untrusted source, delete the e-mail message immediately — without opening or executing any attachments. If the e-mail message is from a trusted source, but you were not expecting an attachment, carefully check the spelling of the e-mail address and contents of the message for errors because perpetrators often make typographical errors. If the message is error-free, verify with the source that he or she intended to send you an attachment — before opening it.

---

**Popular Antivirus Programs**

- AVG Anti-Virus
- avast! antivirus
- CA Anti-Virus
- F-Secure Anti-Virus
- Kaspersky Anti-Virus
- McAfee VirusScan
- Norton AntiVirus
- Trend Micro AntiVirus
- Vexira AntiVirus

---

**Figure 11-4** Many application programs, such as Microsoft Word, can be configured to display a warning if a user attempts to open a file that contains a macro.

**Figure 11-5** Popular antivirus programs.
important activity allows the antivirus program to protect against viruses written since the antivirus program was released and/or its last update. Most antivirus programs contain an automatic update feature that regularly prompts users to download the virus signature, usually at least once a week. The vendor usually provides this service to registered users at no cost for a specified time.

Another technique that antivirus programs use to detect viruses is to inoculate existing program files. To inoculate a program file, the antivirus program records information such as the file size and file creation date in a separate inoculation file. The antivirus program then uses this information to detect if a virus tampers with the data describing the inoculated program file.

If an antivirus program identifies an infected file, it attempts to remove the malware. If the antivirus program cannot remove the infection, it often quarantines the infected file. A quarantine is a separate area of a hard disk that holds the infected file until the infection can be removed. This step ensures other files will not become infected. Users also can quarantine suspicious files themselves. Quarantined files remain on your computer until you delete them or restore them. Restore a quarantined file only if you are certain the antivirus program has removed the infection from the quarantined file.

In extreme cases, you may need to reformat the hard disk to remove malware from an infected computer. Having uninfected, or clean, backups of all files is important. In addition to an antivirus program, users often install a personal firewall program to protect a computer and its data from unauthorized intrusions. Later sections in this chapter discuss backup techniques and firewalls.

Finally, stay informed about new virus alerts and virus hoaxes. A virus hoax is an e-mail message that warns users of a nonexistent virus or other malware. Often, these hoaxes are in the form of a chain letter that requests the user to send a copy of the e-mail message to as many people as possible. The content of the hoax message, for example, may inform users that an important operating system file on their computer is a virus and encourage them to delete the file, which could make their computer unusable. Instead of forwarding the message, visit a Web site that publishes a list of virus alerts and virus hoaxes.

The list in Figure 11-7 summarizes important tips for protecting your computer from viruses and other malware.
Botnets

A botnet is a group of compromised computers connected to a network such as the Internet that are used as part of a network that attacks other networks, usually for nefarious purposes. A compromised computer, known as a zombie, is one whose owner is unaware the computer is being controlled remotely by an outsider.

A bot is a program that performs a repetitive task on a network. Cybercriminals install malicious bots on unprotected computers to create a botnet, also called a zombie army. The perpetrator then uses the botnet to send spam via e-mail, spread viruses and other malware, or commit a distributed denial of service attack, which is discussed in the next section.

FAQ 11-2

How can I tell if my computer is a zombie or in a botnet?
The number of zombie computers is increasing at a rapid rate. Your computer may be a zombie or part of a botnet if you notice unusually high disk activity, a slower than normal Internet connection, or devices connected to your computer becoming increasingly unresponsive. The chances of your computer being a zombie or part of a botnet greatly increase if you do not have an effective firewall.

For more information, visit scsite.com/dc2011/ch11/faq and then click Zombies and Botnets.

Denial of Service Attacks

A denial of service attack, or DoS attack, is an assault whose purpose is to disrupt computer access to an Internet service such as the Web or e-mail. Perpetrators carry out a DoS attack in a variety of ways. For example, they may use an unsuspecting computer to send an influx of confusing data messages or useless traffic to a computer network. The victim computer network slows down considerably and eventually becomes unresponsive or unavailable, blocking legitimate visitors from accessing the network.

A more devastating type of DoS attack is the DDoS (distributed DoS) attack, in which a zombie army is used to attack computers or computer networks. DDoS attacks have been able to stop operations temporarily at numerous Web sites, including powerhouses such as Yahoo!, eBay, Amazon.com, and CNN.com. Read Ethics & Issues 11-1 for a related discussion.

The damage caused by a DoS or DDoS attack usually is extensive. During the outage, retailers lose sales from customers, news sites and search engines lose revenue from advertisers, and time-sensitive information may be delayed. Repeated attacks could tarnish reputations, causing even greater losses.

Perpetrators have a variety of motives for carrying out a DoS or DDoS attack. Those who disagree with the beliefs or actions of a particular organization claim political anger motivates their attacks. Some perpetrators use the attack as a vehicle for extortion. Others simply want the recognition, even though it is negative.

ETHICS & ISSUES 11-1

How Should Cybercriminals Be Punished?
Recenty, a hacker was sentenced to 41 months in jail for illegally using hundreds of a company’s computers as part of a money-making botnet. The punishment is about the same for auto theft, despite the hundreds of thousands of dollars in damages caused in addition to the thousands of dollars the scheme netted the criminal. Viruses, DoS attacks, adware, and other malware continue to disrupt businesses and cause damages that are difficult to estimate.

Many experts and computer administrators claim that the punishment for cybercrime often is out of proportion with the damages caused by the crime. Some legal experts claim that lax security on the part of Internet users is to blame, and perhaps those who practice lax security should be punished as well. Others claim that many organizations provide exorbitant estimates of true damages that cybercriminals cause and that these alleged damages provoke an emotional overreaction to the crimes. The types of crimes and international extent of possible damages are relatively new territories in criminal law.

Should the government create new laws specifically aimed at punishing cybercriminals? Why or why not? Should cybercriminals be punished in proportion to the alleged damages that they cause? Why or why not? Who should decide the extent of the true damages caused by a cybercrime? Why?

Back Doors

A back door is a program or set of instructions in a program that allow users to bypass security controls when accessing a program, computer, or network. Once perpetrators gain access to unsecure computers, they often install a back door or modify an existing program to include a back door, which allows them to continue to access the computer remotely without the user's knowledge. A rootkit can be a back door. Some worms leave back doors, which have been used to spread other worms or to distribute junk e-mail from the unsuspecting victim computers.
Programmers often build back doors into programs during system development. These back doors save development time because the programmer can bypass security controls while writing and testing programs. Similarly, a computer repair technician may install a back door while troubleshooting problems on a computer. If a programmer or computer repair technician fails to remove a back door, a perpetrator could use the back door to gain entry to a computer or network.

**Spoofing**

Spoofing is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network. Several types of spoofing schemes exist. One type, called e-mail spoofing, occurs when the sender's address or other components of the e-mail header are altered so that it appears the e-mail originated from a different sender. E-mail spoofing commonly is used for virus hoaxes, spam, and phishing scams; the latter two are discussed later in the chapter.

Another type, called IP spoofing, occurs when an intruder computer fools a network into believing its IP address is associated with a trusted source. Perpetrators of IP spoofing trick their victims into interacting with the phony Web site. For example, the victim may provide confidential information or download files containing viruses, worms, or other malware.

**Safeguards against Botnets, DoS/DDoS Attacks, Back Doors, and Spoofing**

Some of the latest antivirus programs include provisions to protect a computer from DoS and DDoS attacks. To further defend against these and other Internet and network attacks, users can implement firewall solutions, install intrusion detection software, and set up honeypots.

**Firewalls**

A firewall is hardware and/or software that protects a network’s resources from intrusion by users on another network such as the Internet (Figure 11-8). All networked and online computer users should implement a firewall solution.
Organizations use firewalls to protect network resources from outsiders and to restrict employees’ access to sensitive data such as payroll or personnel records. They can implement a firewall solution themselves or outsource their needs to a company specializing in providing firewall protection.

Large organizations often route all their communications through a proxy server, which typically is a component of the firewall. A proxy server is a server outside the organization’s network that controls which communications pass into the organization’s network. That is, a proxy server carefully screens all incoming and outgoing messages. Proxy servers use a variety of screening techniques. Some check the domain name or IP address of the message for legitimacy. Others require that the messages have digital signatures. A section later in this chapter discusses digital signatures.

Home and small office/home office users often protect their computers with a personal firewall. As discussed in Chapter 8, a personal firewall is a utility program that detects and protects a personal computer and its data from unauthorized intrusions. Personal firewalls constantly monitor all transmissions to and from the computer and may inform a user of any attempted intrusion. Some operating systems, such as Windows, include personal firewalls. For enhanced firewall protection, many users purchase stand-alone personal firewall software (Figure 11-9), usually for less than $50. Many new computers include a free trial version of antivirus software, a personal firewall, and other similar software. To learn more about how to use the Windows firewall, complete the Learn How To 2 activity on page 603.

Some small office/home office users purchase a hardware firewall, such as a router or other device that has a built-in firewall, in addition to or instead of personal firewall software. Hardware firewalls stop intrusions before they attempt to affect your computer maliciously.

Intrusion Detection Software

To provide extra protection against hackers and other intruders, large organizations may use intrusion detection software to identify possible security breaches. Intrusion detection software automatically analyzes all network traffic, assesses system vulnerabilities, identifies any unauthorized intrusions, and notifies network administrators of suspicious behavior patterns or system breaches.

To utilize intrusion detection software requires the expertise of a network administrator because the programs are complex and difficult to use and interpret. These programs also are quite expensive. This software, however, when combined with a firewall, provides an added layer of protection to companies with highly sensitive data such as credit card databases.

Honeypots

Some organizations use honeypots so that they can analyze an attack being perpetrated. A honeypot is a vulnerable computer that is set up to entice an intruder to break into it. These computers, which appear real to the intruder, actually are separated safely from the organization’s network. Honeypots allow the organization to learn how intruders are exploiting their network and also attempt to catch perpetrators who have been doing damage elsewhere on their network. Large Web hosting companies, such as Yahoo! and AT&T, law enforcement agencies, and computer security researchers often use honeypots.

Unauthorized Access and Use

Another type of computer security risk is unauthorized access and use. Unauthorized access is the use of a computer or network without permission. Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities. Unauthorized use includes a variety of activities: an employee using an organization’s computer to send personal e-mail messages, an employee using the organization’s word processing software to track his or her child’s soccer league scores, or someone gaining access to a bank computer and performing an unauthorized transfer. For the home user, most unauthorized use occurs on computers that have always-on Internet connections, such as through Internet cable or DSL.
Safeguards against Unauthorized Access and Use

Organizations take several measures to help prevent unauthorized access and use. At a minimum, they should have a written acceptable use policy (AUP) that outlines the computer activities for which the computer and network may and may not be used. An organization’s AUP should specify the acceptable use of computers by employees for personal reasons. Some organizations prohibit such use entirely. Others allow personal use on the employee’s own time such as a lunch hour. Whatever the policy, an organization should document and explain it to employees.

To protect your personal computer from unauthorized intrusions, you should disable file and printer sharing on your Internet connection (Figure 11-10). This security measure attempts to ensure that others cannot access your files or your printer. To open the window shown in Figure 11-10 in Windows 7, click the Start button on the taskbar, click Control Panel on the Start menu, and then click the ‘Choose homegroup and sharing options’ link in the Network and Internet area of the dialog box.

Other measures that safeguard against unauthorized access and use include firewalls and intrusion detection software, which were discussed in the previous section, and identifying and authenticating users.

Identifying and Authenticating Users

Many organizations use access controls to minimize the chance that a perpetrator intentionally may access or an employee accidentally may access confidential information on a computer. An access control is a security measure that defines who can access a computer, when they can access it, and what actions they can take while accessing the computer. In addition, the computer should maintain an audit trail that records in a file both successful and unsuccessful access attempts. An unsuccessful access attempt could result from a user mistyping his or her password, or it could result from a hacker trying thousands of passwords.

Organizations should investigate unsuccessful access attempts immediately to ensure they are not intentional breaches of security. They also should review successful access for irregularities, such as use of the computer after normal working hours or from remote computers. In addition, an organization regularly should review users’ access privilege levels to determine whether they still are appropriate.

Many systems implement access controls using a two-phase process called identification and authentication. Identification verifies that an individual is a valid user. Authentication verifies that the individual is the person he or she claims to be. Three methods of identification and authentication include user names and passwords, possessed objects, and biometric devices. The technique(s) an organization uses should correspond to the degree of risk that is associated with the unauthorized access. The next sections discuss each of the identification and authentication methods.
User Names and Passwords  A user name, or user ID (identification), is a unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user. A password is a private combination of characters associated with the user name that allows access to certain computer resources.

Most multiuser (networked) operating systems require that users correctly enter a user name and a password before they can access the data, information, and programs stored on a computer or network. Many other systems that maintain financial, personal, and other confidential information also require a user name and password as part of their logon procedure (Figure 11-11).

Some systems assign a user name or user ID to each user. For example, a school may use the student identification number as a user ID. Some Web sites use your e-mail address as the user ID. With other systems, users select their own user name or user ID. Many users select a combination of their first and last names.

Most systems require that users select their own passwords. If a program or device has a default or preset password, such as admin, be sure to change it to prevent unauthorized access. Users typically choose an easy-to-remember word or series of characters for passwords. If your password is too obvious, however, such as your initials or birthday, others can guess it easily.

Easy passwords make it simple for hackers and other intruders to break into a system. Hackers often use computer automated tools to assist them with guessing passwords. Thus, you should select a password carefully. Longer passwords provide greater security than shorter ones. Each character added to a password significantly increases the number of possible combinations and the length of time it might take for someone or a hacker's computer to guess the password (Figure 11-12).

Passwords typically range from 6 to 16 characters. In addition to a user name and password, some systems ask users to enter one of several pieces of personal information. Such items can include a spouse's first name, a birth date, a place of birth, or a mother's maiden name. As with a password, if the user's response does not match information on file, the system denies access.

Instead of passwords, some organizations use passphrases to authenticate users. A passphrase is a private combination of words, often containing mixed capitalization and punctuation, associated with a user name that allows access to certain computer resources. Passphrases, which

<table>
<thead>
<tr>
<th>Number of Characters</th>
<th>Possible Combinations</th>
<th>AVERAGE TIME TO DISCOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Human</td>
</tr>
<tr>
<td>1</td>
<td>36</td>
<td>3 minutes</td>
</tr>
<tr>
<td>2</td>
<td>1,300</td>
<td>2 hours</td>
</tr>
<tr>
<td>3</td>
<td>47,000</td>
<td>3 days</td>
</tr>
<tr>
<td>4</td>
<td>1,700,000</td>
<td>3 months</td>
</tr>
<tr>
<td>5</td>
<td>60,000,000</td>
<td>10 years</td>
</tr>
<tr>
<td>10</td>
<td>3,700,000,000,000,000</td>
<td>580 million years</td>
</tr>
</tbody>
</table>

- Possible characters include the letters A–Z and numbers 0–9
- Human discovery assumes 1 try every 10 seconds
- Computer discovery assumes 1 million tries per second
- Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations
often can be up to 100 characters in length, are more secure than passwords, yet can be easy to remember because they contain words.

Some Web sites use a CAPTCHA to further protect a user’s password. A CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, is a program developed at Carnegie Mellon University to verify that user input is not computer generated. A CAPTCHA displays a series of distorted characters and requires the user enter the characters correctly to continue using the Web site (Figure 11-13). For visually impaired users, the CAPTCHA text can be read aloud. Because unscrupulous individuals attempt to circumvent or decode CAPTCHAs, developers continually are seeking ways to make them more secure or develop alternative authentication techniques. Read Innovative Computing 11-1 to find out how CAPTCHA digitizes newspapers and books.

More than 47,000 editions of The New York Times were published from 1851 to 1980, and a major movement is underway to digitize each paper by scanning every page. Occasionally, the computer cannot decipher a faded or blurry word. When this occurs, the actual image, called a RECAPTCHA, is given an identification number and placed on a Web site such as Ticketmaster, Craigslist, Twitter, LastFM, and Facebook. Visitors must type the correct letters that appear in two images in order to enter the site. When they do, the deciphered words are placed back in their original location in the article being digitized.

Carnegie-Mellon Professor Luis von Ahn created RECAPTCHAs to digitize the millions of words printed in the Times’ archives. He estimates that people worldwide type up to 16 million RECAPTCHAs each day in 1.9 seconds with 100 percent accuracy. Each word has six to eight characters.

In 2000, von Ahn developed single-word CAPTCHAs in an effort to prevent spammers from attacking the Yahoo! Web site. He expanded the venture to help various humanitarian projects, including the Internet Archive, which uses RECAPTCHAs to digitize books.

For more information, visit scsite.com/dc2011/ch11/innovative and then click RECAPTCHA.

FAQ 11-3

How can I protect my password?

Once you select a password, change it frequently. Do not disclose it to anyone or write it on a slip of paper kept near the computer, especially taped to the monitor or under the keyboard. E-mail and telemarketing scams often ask unsuspecting users to disclose their password, so be wary if you did not initiate the inquiry or telephone call. One research study indicates that having too many passwords might compromise security. The average person can remember approximately two secure passwords. Using more than two passwords results in an increased number of calls to the Help desk to reset lost or forgotten passwords.

For more information, visit scsite.com/dc2011/ch11/faq and then click Protecting Passwords.
Possessed Objects  A **possessed object** is any item that you must carry to gain access to a computer or computer facility. Examples of possessed objects are badges, cards, smart cards, and keys. The card you use in an automated teller machine (ATM) is a possessed object that allows access to your bank account.

Possessed objects often are used in combination with personal identification numbers. A **personal identification number (PIN)** is a numeric password, either assigned by a company or selected by a user. PINs provide an additional level of security. An ATM card typically requires a four-digit PIN. Most debit cards and some credit cards use PINs. If someone steals these cards, the thief must enter the user’s PIN to access the account. PINs are passwords. Select them carefully and protect them as you do any other password.

**Biometric Devices**  As Chapter 5 discussed, a **biometric device** authenticates a person’s identity by translating a personal characteristic, such as a fingerprint, into a digital code that is compared with a digital code stored in the computer verifying a physical or behavioral characteristic. If the digital code in the computer does not match the personal characteristic code, the computer denies access to the individual.

Biometric devices grant access to programs, computers, or rooms using computer analysis of some biometric identifier. Examples of biometric devices and systems include fingerprint readers (Figure 11-14), hand geometry systems, face recognition systems, voice verification systems, signature verification systems, iris recognition systems, and retinal scanners. For a more technical discussion about biometrics, specifically fingerprint readers, read the High-Tech Talk article on page 288 in Chapter 5.

Biometric devices are gaining popularity as a security precaution because they are a virtually foolproof method of identification and authentication (read Ethics & Issues 11-2 for a related discussion). For example, many grocery stores, retail stores, and gas stations now use **biometric payment**, where the customer’s fingerprint is read by a fingerprint reader that is linked to a payment method such as a checking account or credit card. Users can forget their user names and passwords. Possessed objects can be lost, copied, duplicated, or stolen. Personal characteristics, by contrast, are unique and cannot be forgotten or misplaced.

Biometric devices do have disadvantages. If you cut your finger, a fingerprint reader might reject you as a legitimate user. Hand geometry readers can transmit germs. If you are nervous, a signature might not match the one on file. If you have a sore throat, a voice recognition system might reject you. Many people are uncomfortable with the thought of using an iris scanner.

**ETHICS & ISSUES 11-2**

**Should You Be Concerned about the Use of Biometric Devices in Public Places?**

Hundreds of thousands of students use a biometric thumbprint to pay for their school lunches each day. School administrators cite the need for biometrics to better track the number of free and subsidized lunches that the schools provide. In an attempt to increase security and track attendance, many school districts require thumbprint identification to enter classrooms or participate in school activities. Retail stores, theme parks, and even physicians’ offices use biometric devices to identify customers and patients. Some privacy advocates believe that the devices store too much personal information. Many are concerned that individuals’ habits more easily can be tracked and then used against them in the future, or that the information could end up in the wrong hands. Some health experts are concerned about the sanitary issue of people passing germs to each other over the biometric devices.

Should children be required to provide biometric information to engage in common public school-related activities? Why or why not? Should anyone who provides products and services be allowed to collect biometric information from a customer? Why or why not? What are the privacy and sanitary issues involved and should they be a concern?
A digital forensics examiner must have knowledge of the law, technical experience with many types of hardware and software products, superior communication skills, familiarity with corporate structures and policies, a willingness to learn and update skills, and a knack for problem solving. For more information about digital forensics, read the Digital Forensics Special Feature that follows this chapter. For a look at the next generation of forensics, read Looking Ahead 11-1.

Digital Forensics
Digital forensics, also called computer forensics, network forensics, or cyberforensics, is the discovery, collection, and analysis of evidence found on computers and networks. Digital forensics involves the examination of computer media, programs, data and log files on computers, servers, and networks. Many areas use digital forensics, including law enforcement, criminal prosecutors, military intelligence, insurance agencies, and information security departments in the private sector.

How many people are victims of identity theft each year?
Studies reveal that identity theft is the fastest growing crime in the United States. In fact, identity theft costs banks, victims, and the government millions of dollars each year, with that amount continually increasing. The chart to the right illustrates the reported number of identity theft cases grouped by age.

FAQ 11-4

Identity Theft — Complaints by Victim Age

Brain Waves, Behavior Tracked to Prevent and Solve Crimes
The brain may one day become part of a crime scene investigation. When a person has committed a criminal or fraudulent act, his brain generates unique waves involuntarily when confronted with pictures, sounds, and words related to the crime scene. Computers can capture and analyze this brain fingerprint of distinctive brain waves to determine if a person has stored critical details of a particular felony or misdemeanor situation.

Similarly, behavior detection systems study a person’s body language, facial expressions, speech, and emotions to isolate specific patterns that criminals commonly exhibit. The surveillance systems can recognize microexpressions, which are the split-second emotions lasting one-fifteenth of a second, on a person’s face.

The U.S. Department of Homeland Security is testing its Future Attribute Screening Technologies (FAST) program, which uses cameras, infrared heat sensors, and lasers to measure pulse and breathing rates. The trial technology is being tested for use at airports and sporting and music events.

Instructions: Find the true statement below. Then, rewrite the remaining false statements so that they are true.

1. A back door attack is an assault whose purpose is to disrupt computer access to an Internet service such as the Web or e-mail.
2. All networked and online computer users should implement a firewall solution.
3. A biometric device translates a personal characteristic into an analog code that is compared with a digital code stored in the computer.
4. Computer viruses, worms, Trojan horses, and rootkits are malware that acts with a user’s knowledge.
5. Perpetrators of cybercrime and other intrusions fall into seven basic categories: hacker, cracker, CERT/CC, corporate spy, unethical employee, trusted source, and cyberterrorist.
6. Shorter passwords provide greater security than longer ones.
7. Updating an antivirus program’s quarantine protects a computer against viruses written since the antivirus program was released.

Quiz Yourself Online: To further check your knowledge of pages 556 through 569, visit scsite.com/dc2011/ch11/quiz and then click Objectives 1 – 3.
Hardware Theft and Vandalism

Hardware theft and vandalism are other types of computer security risks. **Hardware theft** is the act of stealing computer equipment. **Hardware vandalism** is the act of defacing or destroying computer equipment. Hardware vandalism takes many forms, from someone cutting a computer cable to individuals breaking into a business or school computer lab and aimlessly smashing computers.

Hardware theft and vandalism do not really pose a threat to the home desktop computer user. Companies, schools, and other organizations that house many computers, however, are at risk of hardware theft and vandalism, especially those that have smaller system units that easily can fit in a backpack or briefcase.

Mobile users also are susceptible to hardware theft. It is estimated that more than 600,000 notebook computers are stolen each year. The size and weight of these computers, especially netbooks, make them easy to steal. Thieves often target notebook computers of company executives, so that they can use the stolen computer to access confidential company information illegally.

In this case, hardware theft is combined with software and information theft.

**Safeguards against Hardware Theft and Vandalism**

To help reduce the chances of theft, companies and schools use a variety of security measures. Physical access controls, such as locked doors and windows, usually are adequate to protect the equipment. Many businesses, schools, and some homeowners install alarm systems for additional security. School computer labs and other areas with a large number of semifrequent users often attach additional physical security devices such as cables that lock the equipment to a desk (Figure 11-15), cabinet, or floor. Small locking devices also exist that require a key to access a hard disk or optical disc drive.

Some businesses use a real time location system (RTLS) to track and identify the location of high-risk or high-value items. One implementation of RTLS places RFID tags in items to be tracked.

Mobile computer users must take special care to protect their equipment. The best preventive measures are common sense and a constant awareness of the risk. Some users attach a physical device such as a cable to lock a mobile computer temporarily to a stationary object. For example, a hotel guest could lock a notebook computer to a desk or table in a hotel room when he or she leaves the room. Other mobile users install a mini-security system in the notebook computer. Some of these security systems shut down the computer and sound an alarm if the computer moves outside a specified distance. Others can be configured to photograph the thieves when they use the computer. Notebook computer security systems and tracking software also can track the location of a stolen notebook computer.

Some notebook computers use passwords, possessed objects, and biometrics as methods of security. When you start up these computers, you must enter a password, slide a card in a card reader, or press your finger on a fingerprint reader before the hard disk unlocks. This type of security does not prevent theft, but it renders the computer useless if it is stolen.

You also can password-protect many portable storage devices such as USB flash drives, smartphones, and other mobile devices. This allows only authorized users to access the device’s data. Some can be set to destroy data if an incorrect password is entered a certain number of times. You usually can instruct the password screen to display your name and telephone number, so that a Good Samaritan can return it to you if lost. Several models also allow you to encrypt data in the device. A later section in this chapter discusses encryption.
Software Theft

Another computer security risk is software theft. Software theft occurs when someone (1) steals software media, (2) intentionally erases programs, (3) illegally copies a program, or (4) illegally registers and/or activates a program.

The first type of software theft involves a perpetrator physically stealing the media that contain the software or the hardware that contains the media, as described in the previous section. For example, an unscrupulous library patron might steal the Encyclopedia Britannica optical disc.

The second type of software theft can occur when a programmer is terminated from, or stops working for, a company. Although the programs are company property, some dishonest programmers intentionally remove or disable the programs they have written from company computers.

The third type of software theft occurs when software is stolen from software manufacturers. This type of theft, called piracy, is by far the most common form of software theft. Software piracy is the unauthorized and illegal duplication of copyrighted software.

The fourth type of software theft involves users illegally obtaining registration numbers and/or activation codes. A program called a keygen, short for key generator, creates software registration numbers and sometimes activation codes. Some unscrupulous individuals create and post keygens so that users can install software without legally purchasing it.

Safeguards against Software Theft

To protect software media from being stolen, owners should keep original software boxes and media in a secure location, out of sight of prying eyes. All computer users should back up their files and disks regularly, in the event of theft. When some companies terminate a programmer or if the programmer quits, they escort the employee off the premises immediately. These companies believe that allowing terminated employees to remain on the premises gives them time to sabotage files and other network procedures.

To protect themselves from software piracy, software manufacturers issue users license agreements. A license agreement is the right to use the software. That is, you do not own the software. The license agreement provides specific conditions for use of the software, which a user must accept before using the software (Figure 11-16). These terms are displayed when you install the software. Use of the software constitutes acceptance of the terms on the user’s part.

The most common type of license included with software purchased by individual users is a single-user license agreement, also called an end-user license agreement (EULA). A single-user license agreement typically includes many of the following conditions that specify a user’s responsibility upon acceptance of the agreement.

- Users are permitted to:
  - Install the software on only one computer.
  - Make one copy of the software as a backup.
  - Give or sell the software to another individual, but only if the software is removed from the user’s computer first.

- Users are not permitted to:
  - Install the software on a network, such as a school computer lab.
  - Give copies to friends and colleagues, while continuing to use the software.
  - Export the software.
  - Rent or lease the software.

Unless otherwise specified by a license agreement, you do not have the right to copy, loan, borrow, rent, or in any way distribute software. Doing so is a violation of copyright law. It also is a federal crime. Despite this, some experts estimate for every authorized copy of software in use, at least one unauthorized copy exists.

Software piracy continues for several reasons. In some countries, legal protection for software does not exist. In other countries, laws rarely are enforced. In addition, many buyers believe they have the right to copy the software for which they pay hundreds, even thousands, of dollars. Finally, software piracy is a fairly simple crime to commit.

Software piracy, however, is a serious offense. For one, it introduces a number of risks into
the software market. It increases the chance of spreading viruses, reduces your ability to receive technical support, and drives up the price of software for all users. Further, software companies take illegal copying seriously. In some cases, offenders have been prosecuted to the fullest extent of the law with penalties including fines up to $250,000 and five years in jail. Read Ethics & Issues 11-3 for a related discussion.

To promote a better understanding of software piracy problems and, if necessary, to take legal action, a number of major worldwide software companies formed the Business Software Alliance (BSA). The BSA operates a Web site and antipiracy hotlines in the United States and more than 40 other countries.

In an attempt to prevent software piracy, Microsoft and other manufacturers have incorporated an activation process into many of their consumer products. During the product activation, which is conducted either online or by telephone, users provide the software product’s 25-character identification number to receive an installation identification number unique to the computer on which the software is installed. Usually, the software does not function or has limited functionality until you activate it via the Internet or telephone.

Many organizations and businesses also have strict written policies governing the installation and use of software and enforce their rules by checking networked or online computers periodically to ensure that all software is licensed properly. If you are not completely familiar with your school or employer’s policies governing installation of software, check with the information technology department or your school’s technology coordinator.

Information Theft

Information theft is yet another type of computer security risk. Information theft occurs when someone steals personal or confidential information. If stolen, the loss of information can cause as much damage as (if not more than) hardware or software theft.

Both business and home users can fall victim to information theft. An unethical company executive may steal or buy stolen information to learn about a competitor. A corrupt individual may steal credit card numbers to make fraudulent purchases. Information theft often is linked to other types of computer crime. For example, an individual first might gain unauthorized access to a computer and then steal credit card numbers stored in a firm’s accounting department.

Information transmitted over networks offers a higher degree of risk because unscrupulous users can intercept it during transmission. Every computer along the path of your data can see what you send and receive. Ironically, though, studies show that the biggest threat to a business’s information is its internal employees.

Safeguards against Information Theft

Most organizations will attempt to prevent information theft by implementing the user identification and authentication controls discussed earlier in this chapter. These controls are best suited for protecting information on computers located on an organization’s premises.

To protect information on the Internet and networks, organizations and individuals use a variety of encryption techniques.

---

**ETHICS & ISSUES 11-3**

**Should Online Auctions Be Liable for Pirated Software Sales?**

Currently, software companies patrol online auction sites looking for pirated copies of their software that might be for sale. When they find such activity, the software company takes legal action against the seller of the pirated software. With the explosion of online auctions, however, the companies are fighting an uphill battle given the amount of time it takes to discover the sales, find the perpetrators, and then individually bring each perpetrator to justice. Many software companies have joined forces to demand that auction sites, such as eBay, legally be held liable for pirated software sold on their Web sites, and they have offered more than 20 suggestions as to how auction sites could better police their Web sites for pirated software. Online auction Web sites claim that the law clearly states they are not responsible for such sales, but that the software companies legally are responsible for controlling pirated sales. For its part, eBay claims already to enforce more than 13,000 rules to check for suspicious activity on its Web site, and offers trademark holders a special program in which they can enroll and have additional rules enforced.

Should online auctions be liable for pirated software sales on their Web sites? Why or why not? Should new or clearer laws be written to force online auctions to check whether software for sale on their Web sites is pirated? Why? Would you purchase software at an online auction being sold at a substantial discount to prices offered elsewhere? Why or why not?
Encryption

Encryption is a process of converting readable data into unreadable characters to prevent unauthorized access. You treat encrypted data just like any other data. That is, you can store it or send it in an e-mail message. To read the data, the recipient must decrypt, or decipher, it into a readable form.

In the encryption process, the unencrypted, readable data is called plaintext. The encrypted (scrambled) data is called ciphertext. An encryption algorithm, or cypher, is a set of steps that can convert readable plaintext into unreadable ciphertext.

Figure 11-17 shows examples of some simple encryption algorithms. Encryption programs typically use more than one encryption algorithm, along with an encryption key. An encryption key is a set of characters that the originator of the data uses to encrypt the plaintext and the recipient of the data uses to decrypt the ciphertext.

Two basic types of encryption are private key and public key. With private key encryption, also called symmetric key encryption, both the originator and the recipient use the same secret key to encrypt and decrypt the data. Public key encryption, also called asymmetric key encryption, uses two encryption keys: a public key and a private key (Figure 11-18). Public key encryption software generates both the private key and the public key. A message encrypted with a public key can be

<table>
<thead>
<tr>
<th>Name</th>
<th>Algorithm</th>
<th>Plaintext</th>
<th>Ciphertext</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transposition</td>
<td>Switch the order of characters</td>
<td>SOFTWARE</td>
<td>OSTFAWER</td>
<td>Adjacent characters swapped</td>
</tr>
<tr>
<td>Substitution</td>
<td>Replace characters with other characters</td>
<td>INFORMATION</td>
<td>WLDIMXQUWIL</td>
<td>Each letter replaced with another</td>
</tr>
<tr>
<td>Expansion</td>
<td>Insert characters between existing characters</td>
<td>USER</td>
<td>UYSYEYRY</td>
<td>Letter Y inserted after each character</td>
</tr>
<tr>
<td>Compaction</td>
<td>Remove characters and store elsewhere</td>
<td>ACTIVATION</td>
<td>ACIVTIN</td>
<td>Every third letter removed (T, A, O)</td>
</tr>
</tbody>
</table>

Figure 11-17 This table shows four simple encryption algorithms. Most encryption keys use a combination of algorithms.

An Example of Public Key Encryption

Step 1
The sender creates a document to be e-mailed to the receiver.

Step 2
The sender uses the receiver’s public key to encrypt a message.

Step 3
The receiver uses his or her private key to decrypt the message.

Step 4
The receiver can read or print the decrypted message.

Figure 11-18 This figure shows an example of public key encryption.
decrypted only with the corresponding private key, and vice versa. The public key is made known to message originators and recipients. For example, public keys may be posted on a secure Web page or a public-key server, or they may be e-mailed. The private key, by contrast, should be kept confidential. For a more technical discussion about encryption algorithms and keys, read the High-Tech Talk article on page 592.

Some operating systems and e-mail programs allow you to encrypt the contents of files and messages that are stored on your computer. You also can purchase an encryption program, such as Pretty Good Privacy (PGP).

A digital signature is an encrypted code that a person, Web site, or organization attaches to an electronic message to verify the identity of the message sender. The code usually consists of the user's name and a hash of all or part of the message. A hash is a mathematical formula that generates a code from the contents of the message. Thus, the hash differs for each message. Receivers of the message decrypt the digital signature. The recipient generates a new hash of the received message and compares it with one in the digital signature to ensure they match.

Digital signatures often are used to ensure that an impostor is not participating in an Internet transaction. That is, digital signatures help to prevent e-mail forgery. A digital signature also can verify that the content of a message has not changed.

Many Web browsers also use encryption. Some browsers offer a protection level known as 40-bit encryption. Many also offer 128-bit encryption and 1024-bit encryption, which are even higher levels of protection because they have longer encryption keys. Applications requiring more security, such as banks, brokerage firms, or online retailers that use credit card or other financial information, require 128-bit or 1024-bit encryption.

A Web site that uses encryption techniques to secure its data is known as a secure site. Secure sites use digital certificates along with a security protocol. Two popular security protocols are Transport Layer Security and Secure HTTP. Organizations often use VPNs. The following paragraphs briefly discuss security techniques.

Digital Certificates A digital certificate is a notice that guarantees a user or a Web site is legitimate. E-commerce applications commonly use digital certificates. Web browsers, such as Internet Explorer, often display a warning message if a Web site does not have a valid digital certificate.

A certificate authority (CA) is an authorized person or a company that issues and verifies digital certificates. Users apply for a digital certificate from a CA (Figure 11-19). A digital certificate typically contains information such as the user's name, the issuing CA's name and signature, and the serial number of the certificate. The information in a digital certificate is encrypted.

For more information, visit scsite.com/dc2011/ch11/weblink and then click Digital Certificates.
Transport Layer Security  

Transport Layer Security (TLS), a successor to Secure Sockets Layer (SSL), provides encryption of all data that passes between a client and an Internet server. TLS requires the client to have a digital certificate. Once the server has a digital certificate, the Web browser communicates securely with the client. TLS prevents perpetrators from accessing or tampering with communications. Web addresses of pages that use TLS typically begin with https, instead of http (Figure 11-20). TLS is available in 128-bit encryption and higher.

Secure HTTP  

Secure HTTP (S-HTTP) allows users to choose an encryption scheme for data that passes between a client and a server. With S-HTTP, the client and server both must have digital certificates. S-HTTP is more difficult to use than TLS, but it is more secure. Applications that must verify the authenticity of a client, such as for online banking, use S-HTTP.

VPN  

Mobile users today often access their company networks through a virtual private network. When a mobile user connects to a main office using a standard Internet connection, a virtual private network (VPN) provides the mobile user with a secure connection to the company network server, as if the user has a private line. VPNs help ensure that data is safe from being intercepted by unauthorized people by encrypting data as it transmits from a notebook computer, smart phone, or other mobile device.

System Failure  

System failure is yet another type of computer security risk. A system failure is the prolonged malfunction of a computer. System failure also can cause loss of hardware, software, data, or information. A variety of causes can lead to system failure. These include aging hardware; natural disasters such as fires, floods, or hurricanes; random events such as electrical power problems; and even errors in computer programs.

One of the more common causes of system failure is an electrical power variation. Electrical power variations can cause loss of data and loss of equipment. If the computer equipment is networked, a single power disturbance can damage multiple systems. Electrical disturbances include noise, undervoltages, and overvoltages.

Noise is any unwanted signal, usually varying quickly, that is mixed with the normal voltage entering the computer. Noise is caused by external devices such as fluorescent lighting, radios, and televisions, as well as by components within the computer itself. Noise generally is not a risk to hardware, software, or data. Computer power supplies, however, do filter out noise.

An undervoltage occurs when the electrical supply drops. In North America, a wall plug usually supplies electricity at approximately 120 volts. An undervoltage occurs when the voltage drops, often defined as more than five percent, below the normal volts. A brownout is a prolonged (more than a minute) undervoltage. A blackout is a complete power failure. Undervoltages can cause data loss but generally do not cause equipment damage.

An overvoltage, or power surge, occurs when the incoming electrical power increases, often defined as more than five percent, above the normal volts. A momentary overvoltage, which is called a spike, occurs when the increase in power lasts for less than one millisecond (one thousandth of a second). Uncontrollable disturbances such as lightning bolts can cause spikes. Overvoltages can cause immediate and permanent damage to hardware.
Safeguards against System Failure

To protect against electrical power variations, use a surge protector. A surge protector, also called a surge suppressor, uses special electrical components to smooth out minor noise, provide a stable current flow, and keep an overvoltage from reaching the computer and other electronic equipment (Figure 11-21). Sometimes resembling a power strip, the computer and other devices plug in the surge protector, which plugs in the power source. The surge protector absorbs small overvoltages — generally without damage to the computer and equipment. To protect the computer and other equipment from large overvoltages, such as those caused by a lightning strike, some surge protectors completely stop working when an overvoltage reaches a certain level. Surge protectors also usually protect the computer from undervoltages.

No surge protectors are 100 percent effective. Large power surges can bypass the protector. Repeated small overvoltages can weaken a surge protector permanently. Some experts recommend replacing a surge protector every two to three years. Typically, the amount of protection offered by a surge protector is proportional to its cost. That is, the more expensive, the more protection the protector offers. Be sure to review the manufacturer's guarantee when purchasing a surge protector. Some will replace equipment damaged by a power surge, if the equipment was connected to their surge protector.

The surge protector you purchase should meet the safety specification for surge suppression products. This specification, which is called the Underwriters Laboratories (UL) 1449 standard, allows no more than 500 maximum volts to pass through the line. The response time of the surge protector should be less than one nanosecond. The surge protector also should have a Joule rating of at least 200. A Joule is the unit of energy a surge protection device can absorb before it can be damaged. The higher the Joule rating, the better the protection.

If your computer connects to a network or the Internet, also be sure to have protection for your modem, telephone lines, DSL lines, Internet cable lines, and network lines. Many surge protectors include plug-ins for telephone lines and other cables. If yours does not, you can purchase separate devices to protect these lines.

For additional electrical protection, some users connect an uninterruptible power supply to the computer. An uninterruptible power supply (UPS) is a device that contains surge protection circuits and one or more batteries that can provide power during a temporary or permanent loss of power (Figure 11-22). A UPS connects between your computer and a power source.

Two types of UPS devices are standby and online. A standby UPS, sometimes called an offline UPS, switches to battery power when a problem occurs in the power line. The amount of time a standby UPS allows a user to continue working depends on the electrical requirements of the computer and the size of the batteries in the UPS. A UPS for a personal computer should provide from 10 to 50 minutes of use in the event of a total power loss. This should
be enough time to save current work and shut down the computer properly. An online UPS always runs off the battery, which provides continuous protection. An online UPS is much more expensive than a standby UPS.

Some companies use duplicate components or computers to protect against system failure. A fault-tolerant computer has duplicate components so that it can continue to operate when one of its main components fail. Companies that must have their computers operational at all times may have two separate duplicate computers running simultaneously. Airline reservation systems, communications networks, and automated teller machines are examples of systems that duplicate components or computers to ensure that no data is lost in the event of a system failure.

**FAQ 11-5**

**Should I use a surge protector on electronic equipment, appliances, or even my entire house?**

It is a good idea to use a surge protector on high-end, expensive electronic equipment such as entertainment systems, DVD/Blu-ray Disc players, computers, and copy machines, and on any household appliance or device that includes a circuit board or computer such as a stove, dishwasher, and microwave. You also can hire an electrician to install a surge protector that protects your entire house. This type of surge protector is installed where the power lines connect to your house's electrical system. A lightning strike or other substantial power surge could damage electrical devices in your house. In addition to protecting the equipment in your house, it also is a good idea to carry a portable surge protector when you travel, so that you can protect your cell phone and other mobile devices when you plug them in to charge.

For more information, visit scsite.com/dc2011/ch11/faq and then click Surge Protectors.

**Backing Up — The Ultimate Safeguard**

To protect against data loss caused by system failure or hardware/software/information theft, computer users should back up files regularly. A backup is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed. Thus, to back up a file means to make a copy of it. In the case of system failure or the discovery of corrupted files, you restore the files by copying the backed up files to their original location on the computer.

You can use just about any media to store backups. Be sure to use high-quality media. A good choice for a home user might be optical discs or external hard disks. Some home users also set up a RAID configuration, as described in Chapter 7, to automatically back up the contents of a disk.

Keep backup copies in a fireproof and heatproof safe or vault, or offsite. Offsite means in a location separate from the computer site. Home and business users keep backup copies offsite so that a single disaster, such as a fire, does not destroy both the original and the backup copy of the data. An offsite location can be a safe deposit box at a bank or a briefcase.

A growing trend is to use cloud storage as an offsite location. As discussed in Chapter 7, cloud storage is an Internet service that provides storage to computer users. To learn more about how to back up files using an Internet service, complete the Learn How To! activity on pages 602 and 603.

Most backup programs for the home user provide for a full backup and a selective backup. A full backup copies all of the files in the computer. With a selective backup, users choose which folders and files to include in a backup.

Some users implement a three-generation backup policy to preserve three copies of important files. The grandparent is the oldest copy of the file. The parent is the second oldest copy of the file. The child is the most recent copy of the file. Others use RAID to duplicate the contents of a disk. Instead of multiple backup copies, some users choose continuous backup, where data is backed up whenever a change is made.

Backup programs are available from many sources. Most operating systems include a backup program. Backup devices, such as external disk drives, also include backup programs. Numerous stand-alone backup utilities exist. Many of these can be downloaded from the Web at no cost.

**Wireless Security**

Wireless technology has made dramatic changes in the way computer users communicate worldwide. Billions of home and business users have notebook computers, smart phones, and other mobile devices to access the Internet, send e-mail and instant messages,
Home users set up wireless home networks. Mobile users access wireless networks in hot spots at airports, hotels, shopping malls, bookstores, restaurants, and coffee shops. Schools have wireless networks so that students can access the school network using their mobile computers and devices as they move from building to building.

Although wireless access provides many conveniences to users, it also poses additional security risks. One study showed that about 80 percent of wireless networks have no security protection. Some perpetrators connect to other’s wireless networks to gain free Internet access; others may try to access an organization’s confidential data.

To access the network, the individual must be in range of the wireless network. Some intruders intercept and monitor communications as they transmit through the air. Others connect to a network through an unsecured wireless access point (WAP). In one technique, called war driving or access point mapping, individuals attempt to detect wireless networks via their note- book computer or mobile device while driving a vehicle through areas they suspect have a wireless network. Some individuals instead use war flying, where they use airplanes instead of vehicles to detect unsecured wireless networks. Once located, some individuals use a GPS device to add the WAP to a war driving access point map on the Internet (Figure 11-23), making the wireless network vulnerable.

In addition to using firewalls, some safeguards that improve the security of wireless networks include reconfiguring the wireless access point and ensuring equipment uses one or more wireless security standards such as Wi-Fi Protected Access and 802.11i.

- A wireless access point (WAP) should be configured so that it does not broadcast a network name, known as an SSID (service set identifier). Users should change the default SSID to prevent unauthorized users from accessing their wireless network. The WAP also can be programmed so that only certain devices can access it.
- Wi-Fi Protected Access (WPA) is a security standard that improves on older security standards by authenticating network users and providing more advanced encryption techniques.
- An 802.11i network, sometimes called WPA2, the most recent network security standard, conforms to the government’s security standards and uses more sophisticated encryption techniques than WPA.

By implementing these security measures, you can help to prevent unauthorized access to wireless networks.

FAQ 11-6

Can you detect if someone is accessing your wireless home network?

Yes. If you notice that the speed of your wireless network connection is slower than normal, it may be a sign that someone else is accessing your network. You also may notice indicator lights on your wireless router flashing rapidly when you are not connected to your wireless network. Most wireless routers have a built-in utility that allows you to view the computers currently connected to your network. If you notice a computer that does not belong to you, consult your wireless router’s documentation to determine how to remove it from the network.

For more information, visit scsite.com/dc2011/ch11/faq and then click Wireless Home Networks.

Figure 11-23 This Web site marks all unsecured wireless networks located during a war drive.
Health Concerns of Computer Use

Users are a key component in any information system. Thus, protecting users is just as important as protecting hardware, software, and data.

The widespread use of computers has led to some important user health concerns. Users should be proactive and minimize their chance of risk. The following sections discuss health risks and preventions, along with measures users can take to keep the environment healthy.

Computers and Health Risks

A repetitive strain injury (RSI) is an injury or disorder of the muscles, nerves, tendons, ligaments, and joints. Computer-related RSIs include tendonitis and carpal tunnel syndrome. RSIs are the largest job-related injury and illness problem in the United States today. For this reason, OSHA (Occupational Safety and Health Administration) has developed industry-specific and task-specific guidelines designed to prevent workplace injuries with respect to computer usage.

Tendonitis is inflammation of a tendon due to repeated motion or stress on that tendon.

Carpal tunnel syndrome (CTS) is inflammation of the nerve that connects the forearm to the palm of the wrist. Repeated or forceful bending of the wrist can cause CTS or tendonitis of the wrist. Symptoms of tendonitis of the wrist include extreme pain that extends from the forearm to the hand, along with tingling in the fingers. Symptoms of CTS include burning pain when the nerve is compressed, along with numbness and tingling in the thumb and first two fingers.

Long-term computer work can lead to tendonitis or CTS. Factors that cause these disorders include prolonged typing, prolonged mouse usage, or continual shifting between the mouse and the keyboard. If untreated, these disorders can lead to permanent physical damage.

You can take many precautions to prevent these types of injuries. Take frequent breaks during the computer session to exercise your hands and arms (Figure 11-24). To prevent injury due to typing, place a wrist rest between the keyboard and the edge of your desk. To prevent injury while using a mouse, place the mouse at least six inches from the edge of the desk. In this position, your wrist is flat on the desk. Finally, minimize the number of times you switch between the mouse and the keyboard, and avoid using the heel of your hand as a pivot point while typing or using the mouse.

Another type of health-related condition due to computer usage is computer vision syndrome (CVS). You may have CVS if you have sore, tired, burning, itching, or dry eyes; blurred or double vision; distance blurred vision after prolonged

Hand Exercises

- Spread fingers apart for several seconds while keeping wrists straight.
- Gently push back fingers and then thumb.
- Dangle arms loosely at sides and then shake arms and hands.

Instructions: Find the true statement below. Then, rewrite the remaining false statements so that they are true.

1. An end-user license agreement (EULA) permits users to give copies to friends and colleagues, while continuing to use the software.
2. Encryption is a process of converting ciphertext into plaintext to prevent unauthorized access.
3. Mobile users are not susceptible to hardware theft.
4. Overvoltages can cause immediate and permanent damage to hardware.
5. Two backup security standards are Wi-Fi Protected Access and 802.11i.
6. To protect against data loss caused by a system failure, computer users should restore files regularly.

Quiz Yourself Online: To further check your knowledge of pages 570 through 578, visit scsite.com/dc2011/ch11/quiz and then click Objectives 4 – 9.
staring at a display device; headache or sore neck; difficulty shifting focus between a display device and documents; difficulty focusing on the screen image; color fringes or after-images when you look away from the display device; and increased sensitivity to light. Eye strain associated with CVS is not thought to have serious or long-term consequences. Figure 11-25 outlines some techniques you can follow to ease eyestrain.

Techniques to Ease Eyestrain
- Every 10 to 15 minutes, take an eye break.
  - Look into the distance and focus on an object for 20 to 30 seconds.
  - Roll your eyes in a complete circle.
  - Close your eyes and rest them for at least one minute.
  - Blink your eyes every five seconds.
  - Place your display device about an arm’s length away from your eyes with the top of the screen at eye level or below.
  - Use large fonts.
  - If you wear glasses, ask your doctor about computer glasses.
  - Adjust the lighting.

People who spend their workday using the computer sometimes complain of lower back pain, muscle fatigue, and emotional fatigue. Lower back pain sometimes is caused from poor posture. Always sit properly in the chair while you work. To alleviate back pain, muscle fatigue, and emotional fatigue, take a 15- to 30-minute break every 2 hours — stand up, walk around, stretch, and relax. Another way to help prevent these injuries is to be sure your workplace is designed ergonomically.

Ergonomics and Workplace Design
Ergonomics is an applied science devoted to incorporating comfort, efficiency, and safety into the design of items in the workplace. Ergonomic studies have shown that using the correct type and configuration of chair, keyboard, display device, and work surface helps users work comfortably and efficiently and helps protect their health. For the computer work space, experts recommend an area of at least two feet by four feet. Figure 11-26 illustrates additional guidelines for setting up the work area.

Figure 11-25 Following these tips may help reduce eyestrain while working on a computer.
Computer Addiction

Computers can provide entertainment and enjoyment. Some computer users, however, become obsessed with the computer and the Internet. **Computer addiction** occurs when the computer consumes someone’s entire social life. Computer addiction is a growing health problem but can be treated through therapy and support groups.

Symptoms of a user with computer addiction include the following:

- Craves computer time
- Overjoyed when at the computer
- Unable to stop computer activity
- Irritable when not at the computer
- Neglects family and friends
- Problems at work or school

Ethics and Society

As with any powerful technology, computers can be used for both good and bad intentions. The standards that determine whether an action is good or bad are known as ethics. **Computer ethics** are the moral guidelines that govern the use of computers and information systems. Seven frequently discussed areas of computer ethics are unauthorized use of computers and networks, software theft (piracy), information accuracy, intellectual property rights, codes of conduct, information privacy, and green computing. The questionnaire in Figure 11-27 raises issues in each of these areas.

Previous sections in this chapter discussed unauthorized use of computers and networks, and software theft (piracy). The following sections

<table>
<thead>
<tr>
<th>Your Thoughts?</th>
<th>Ethical</th>
<th>Unethical</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. An organization requires employees to wear badges that track their whereabouts while at work.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>2. A supervisor reads an employee’s e-mail.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>3. An employee uses his computer at work to send e-mail messages to a friend.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>4. An employee sends an e-mail message to several coworkers and blind copies his supervisor.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>5. An employee forwards an e-mail message to a third party without permission from the sender.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>6. An employee uses her computer at work to complete a homework assignment for school.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>7. The vice president of your Student Government Association (SGA) downloads a photo from the Web and uses it in a flyer recruiting SGA members.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>8. A student copies text from the Web and uses it in a research paper for his English Composition class.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>9. An employee sends political campaign material to individuals on her employer’s mailing list.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>10. As an employee in the registration office, you have access to student grades. You look up grades for your friends, so that they do not have to wait for delivery of grade reports from the postal service.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>11. An employee makes a copy of software and installs it on her home computer. No one uses her home computer while she is at work, and she uses her home computer only to finish projects from work.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>12. An employee who has been laid off installs a computer virus on his employer’s computer.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>13. A person designing a Web page finds one on the Web similar to his requirements, copies it, modifies it, and publishes it as his own Web page.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>14. A student researches using only the Web to write a report.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>15. In a society in which all transactions occur online (a cashless society), the government tracks every transaction you make and automatically deducts taxes from your bank account.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>16. Someone copies a well-known novel to the Web and encourages others to read it.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>17. A person accesses an organization’s network and reports to the organization any vulnerabilities discovered.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>18. Your friend uses a neighbor’s wireless network to connect to the Internet and check e-mail.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>19. A company uses recycled paper to print a 50-page employee benefits manual that is distributed to 425 employees.</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>20. Your friend donates her old computers and mobile devices to local schools when she purchases newer models.</td>
<td>❑</td>
<td>❑</td>
</tr>
</tbody>
</table>

Figure 11-27  Indicate whether you think the situation described is ethical or unethical. Discuss your answers with your instructor and other students.
discuss issues related to information accuracy, intellectual property rights, codes of conduct, green computing, and information privacy.

**Information Accuracy**

Information accuracy today is a concern because many users access information maintained by other people or companies, such as on the Internet. Do not assume that because the information is on the Web that it is correct. As Chapter 2 discussed, users should evaluate the value of a Web page before relying on its content. Be aware that the organization providing access to the information may not be the creator of the information.

In addition to concerns about the accuracy of computer input, some individuals and organizations raise questions about the ethics of using computers to alter output, primarily graphical output such as a retouched photo. Using graphics equipment and software, users easily can digitize photos and then add, change, or remove images (Figure 11-28).

One group that completely opposes any manipulation of an image is the National Press Photographers Association. It believes that allowing even the slightest alteration eventually could lead to misrepresentative photos. Others believe that digital photo retouching is acceptable as long as the significant content or meaning of the photo does not change. Digital retouching is an area in which legal precedents so far have not been established.

**Intellectual Property Rights**

*Intellectual property (IP)* refers to unique and original works such as ideas, inventions, art, writings, processes, company and product names, and logos. *Intellectual property rights* are the rights to which creators are entitled for their work. Certain issues arise surrounding IP today because many of these works are available digitally.

A *copyright* gives authors and artists exclusive rights to duplicate, publish, and sell their materials. A copyright protects any tangible form of expression.

A common infringement of copyright is piracy. People pirate (illegally copy) software, movies, and music. Many areas are not clear-cut with respect to the law, because copyright law gives the public fair use to copyrighted material. The issues surround the phrase, fair use, which allows use for educational and critical purposes. This vague definition is subject to widespread interpretation and raises many questions:

- Should individuals be able to download contents of your Web site, modify it, and then put it on the Web again as their own?
- Should a faculty member have the right to print material from the Web and distribute it to all members of the class for teaching purposes only?
- Should someone be able to scan photos or pages from a book, publish them to the Web, and allow others to download them?
- Should someone be able to put the lyrics of a song on the Web?
- Should students be able to post term papers they have written on the Web, making it tempting for other students to download and submit them as their own work?

These issues with copyright law led to the development of *digital rights management (DRM)*, a strategy designed to prevent illegal distribution of movies, music, and other digital content.

**Codes of Conduct**

Recognizing that individuals need specific standards for the ethical use of computers, a number of computer-related organizations have established IT (information technology) codes of conduct (Figure 11-29). An IT *code of conduct* is a written guideline that helps determine whether a specific computer action is ethical or unethical.
Green Computing

Green computing involves reducing the electricity and environmental waste while using a computer. People use, and often waste, resources such as electricity and paper while using a computer. Society has become aware of this waste and is taking measures to combat it.

Personal computers, display devices, and printers should comply with guidelines of the ENERGY STAR program. The United States Department of Energy (DOE) and the United States Environmental Protection Agency (EPA) developed the ENERGY STAR program to help reduce the amount of electricity used by computers and related devices. This program encourages manufacturers to create energy-efficient devices that require little power when they are not in use.

For example, many devices switch to sleep or power save mode after a specified number of inactive minutes or hours. Computers and devices that meet the ENERGY STAR guidelines display an ENERGY STAR label.

A recent study showed that organizational computer facilities, or data centers, in the United States consumed as much power as about six million households, and if no measures are taken to reduce consumption, the number is expected to continue rising quickly. Data center resources that consume power include computer hardware and associated devices, uninterruptible power supplies, and utilities such as air conditioning, coolers, lighting, etc. Organizations can implement a variety of measures to reduce electrical waste.

• Consolidate servers by using virtualization (discussed in Chapter 8)
• Purchase high-efficiency equipment, such as uninterruptible power supplies and storage devices
• Use sleep modes and other power management features for computers and devices
• Buy computers with low power consumption processors and power supplies
• When possible, use outside air to cool the data center

Some organizations continually review their power usage effectiveness (PUE), which is a ratio that measures how much power enters the computer facility, or data center, against the amount of power required to run the computers.

Users should not store obsolete computers and devices in their basement, storage room, attic, warehouse, or any other location. Computers, monitors, and other equipment contain toxic materials and potentially dangerous elements including lead, mercury, and flame retardants. In a landfill, these materials release into the environment. Recycling and refurbishing old equipment are much safer alternatives for the environment. Manufacturers can use the millions of pounds of recycled raw materials to make products such as outdoor furniture and automotive parts.

Experts estimate that more than 700 million personal computers are obsolete. Because of the huge volumes of electronic waste, the U.S. federal government has proposed a bill that would require computer recycling across the country. Many state and local governments have methods in place to make it easy for consumers to recycle this type of equipment. Many computer manufacturers, office supply stores, and other agencies offer free recycling to consumers and organizations.

IT Code of Conduct

1. Computers may not be used to harm other people.
2. Employees may not interfere with others’ computer work.
3. Employees may not meddle in others’ computer files.
4. Computers may not be used to steal.
5. Computers may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others’ computer resources without authorization.
8. Employees may not use others’ intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use computers in a way that demonstrates consideration and respect for fellow humans.

Figure 11-29  Sample IT code of conduct employers may distribute to employees.
To reduce the environmental impact of computing further, users simply can alter a few habits. Figure 11-30 lists the ways you can contribute to green computing. To learn more about green computing, complete the Green Computing exercise on the Web Research page in each chapter of this book.

Figure 11-30  A list of suggestions to make computing healthy for the environment.

**Green Computing Suggestions**

1. Use computers and devices that comply with the ENERGY STAR program.
2. Do not leave the computer running overnight.
3. Turn off the monitor, printer, and other devices when not in use.
4. Use LCD monitors instead of CRT monitors.
5. Use paperless methods to communicate.
6. Recycle paper.
7. Buy recycled paper.
8. Recycle toner cartridges.
9. Recycle old computers, printers, and other devices.
10. Telecommute to save gas.
11. Use video conferencing and VoIP for meetings.

**How to Safeguard Personal Information**

1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your telephone number or Social Security number on personal checks.
3. Have an unlisted or unpublished telephone number.
4. If Caller ID is available in your area, find out how to block your number from displaying on the receiver’s system.
5. Do not write your telephone number on charge or credit receipts.
6. Ask merchants not to write credit card numbers, telephone numbers, Social Security numbers, and driver’s license numbers on the back of your personal checks.
7. Purchase goods with cash, rather than credit or checks.
8. Avoid shopping club and buyer cards.
9. If merchants ask personal questions, find out why they want to know before releasing the information.
10. Inform merchants that you do not want them to distribute your personal information.
11. Request, in writing, to be removed from mailing lists.
12. Obtain your credit report once a year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) and correct any errors.
13. Request a free copy of your medical records once a year from the Medical Information Bureau.
14. Limit the amount of information you provide to Web sites. Fill in only required information.
15. Install a cookie manager to filter cookies.
16. Clear your history file when you are finished browsing.
17. Set up a free e-mail account. Use this e-mail address for merchant forms.
18. Turn off file and printer sharing on your Internet connection.
19. Install a personal firewall.
20. Sign up for e-mail filtering through your Internet access provider or use an anti-spam program such as Brightmail.
21. Do not reply to spam for any reason.
22. Surf the Web anonymously with a program such as Freedom WebSecure or through an anonymous Web site such as Anonymizer.com.

**Information Privacy**

*Information privacy* refers to the right of individuals and companies to deny or restrict the collection and use of information about them. In the past, information privacy was easier to maintain because information was kept in separate locations. Each retail store had its own credit files. Each government agency maintained separate records. Doctors had their own patient files.

Today, huge databases store this data online. Much of the data is personal and confidential and should be accessible only to authorized users. Many individuals and organizations, however, question whether this data really is private. That is, some companies and individuals collect and use this information without your authorization. Web sites often collect data about you, so that they can customize advertisements and send you personalized e-mail messages. Some employers monitor your computer usage and e-mail messages.

Figure 11-31  Techniques to keep personal data private.
Electronic Profiles
When you fill out a form such as a magazine subscription, product warranty registration card, or contest entry form, the merchant that receives the form usually enters it into a database. Likewise, every time you click an advertisement on the Web or register software online, your information and preferences enter a database. Merchants then sell the contents of their databases to national marketing firms and Internet advertising firms. By combining this data with information from public sources such as driver’s licenses and vehicle registrations, these firms create an electronic profile of individuals. The information in these electronic profiles includes personal details such as your age, address, telephone number, spending habits, marital status, number of dependents, ages of dependents, and so on.

Direct marketing supporters say that using information in this way lowers overall selling costs, which lowers product prices. Critics contend that the information in an electronic profile reveals more about an individual than anyone has a right to know. They claim that companies should inform people if they plan to provide personal information to others, and people should have the right to deny such use. Many companies today allow people to specify whether they want their personal information distributed (Figure 11-32).

Cookies
E-commerce and other Web applications often rely on cookies to identify users and customize Web pages. A cookie is a small text file that a Web server stores on your computer. Cookie files typically contain data about you, such as your user name or viewing preferences.
Web sites use cookies for a variety of purposes:

- Most Web sites that allow for personalization use cookies to track user preferences. On such sites, users may be asked to fill in a form requesting personal information, such as their name, postal code, or site preferences. A news Web site, for example, might allow users to customize their viewing preferences to display certain stock quotes or the local weather forecast. The Web site stores their preferences in a cookie on the users’ hard disks.

- Some Web sites use cookies to store users’ passwords, so that they do not need to enter it every time they log in to the Web site.

- Online shopping sites generally use a session cookie to keep track of items in a user’s shopping cart. This way, users can start an order during one Web session and finish it on another day in another session. Session cookies usually expire after a certain time, such as a week or a month.

- Some Web sites use cookies to track how often users visit a site and the Web pages they visit while at the site.

- Web sites may use cookies to target advertisements. These sites store a user’s interests and browsing habits in the cookie.

Many commercial Web sites send a cookie to your browser, and then your computer’s hard disk stores the cookie. The next time you visit the Web site, your browser retrieves the cookie from your hard disk and sends the data in the cookie to the Web site. Figure 11-33 illustrates how Web sites work with cookies. A Web site can read data only from its own cookie file stored on your hard disk. That is, it cannot access or view any other data on your hard disk — including another cookie file.

Some Web sites do sell or trade information stored in your cookie to advertisers — a practice many believe to be unethical. If you do not want your personal information distributed, you should limit the amount of information you provide to a Web site.

**Figure 11-33** This figure shows how cookies work.
You can set your browser to accept cookies automatically, prompt you if you want to accept a cookie, or disable cookie use altogether. Keep in mind if you disable cookie use, you may not be able to use many of the e-commerce Web sites. As an alternative, you can purchase software that selectively blocks cookies.

**Spam**

Spam is an unsolicited e-mail message or newsgroup posting sent to many recipients or newsgroups at once. Spam is Internet junk mail (Figure 11-34). The content of spam ranges from selling a product or service, to promoting a business opportunity, to advertising offensive material. One study indicates more than 92 percent of e-mail is spam. Instead of via e-mail, some spam is sent through an instant messaging system and, thus, is called spim. Another type, called spit, is spam sent via VoIP.

Users can reduce the amount of spam they receive with a number of techniques. Some e-mail programs have built-in settings that allow users to delete spam automatically. Users also can sign up for e-mail filtering from their Internet access provider. **E-mail filtering** is a service that blocks e-mail messages from designated sources. These services typically collect the spam in a central location that users can view at any time. An alternative to e-mail filtering is to purchase an **anti-spam program** that attempts to remove spam before it reaches your inbox. The disadvantage of e-mail filters and anti-spam programs is that sometimes they remove valid e-mail messages. Thus, users should review the contents of the spam messages periodically to ensure they do not contain valid messages.

**Phishing**

Phishing is a scam in which a perpetrator sends an official looking e-mail message that attempts to obtain your personal and financial information (Figure 11-35). Some phishing e-mail messages ask you to reply with your information; others direct you to a phony Web site, or a pop-up window that looks like a Web site, that collects the information.

If you receive an e-mail message that looks legitimate and requests you update credit card numbers, Social Security numbers, bank account numbers, passwords, or other private information, the FTC recommends you visit the Web site directly to determine if the request is valid.

---

**FAQ 11-7**

**How prevalent is spam?**

The amount of spam on the Internet has continued to increase for several years. One research study indicates that during one three-month period, more than 92 percent of all e-mail messages were spam. The study also estimates that the United States relays more spam than any other country.

For more information, visit scsite.com/dc2011/ch11/faq and then click Spam.
Chapter 11 Computer Security and Safety, Ethics, and Privacy

588

contain sender identification so that recipients can verify the legitimacy of messages. Read Ethics & Issues 11-4 for a related discussion.

Phishing is a scam, similar to phishing, where a perpetrator attempts to obtain your personal and financial information, except they do so via spoofing. That is, when you type a Web address in the Web browser, you are redirected to a phony Web site that looks legitimate. The phony Web site requests you enter confidential information.

Clickjacking is yet another similar scam. With clickjacking, an object that can be clicked on a Web site, such as a button, image, or link, contains a malicious program. When a user clicks the disguised object, a variety of nefarious events may occur. For example, the user may be redirected to a phony Web site that requests personal information, or a virus may download to the computer.

FAQ 11-8

What do I do if I have been caught in a phishing scam?

If you have been trapped in a phishing scam, immediately change any passwords that may have been compromised. If you have disclosed your debit or credit card numbers, contact your financial institutions. You also should visit http://www.ftc.gov or call the FTC help line at this number: 1-877-FTC-HELP. If you are an employee and suspect that confidential information about your organization has been compromised, immediately notify your supervisor.

Spyware and Adware

Recall from Chapter 8 that spyware is a program placed on a computer without the user's knowledge that secretly collects information about the user. Some vendors or employers use spyware to collect information about program usage or employees. Internet advertising firms often collect information about users' Web browsing habits by hiding spyware in adware. Adware is a program that displays online advertisements in a banner or pop-up window on Web pages, e-mail messages, or other Internet services.

Another type of spyware, called a Web bug, is hidden on Web pages or in e-mail messages in the form of graphical images. Web businesses use Web bugs to monitor online habits of Web site visitors. Often, Web bugs link to a cookie stored on the hard disk. (Cookies are not considered spyware because you know they exist.)

To remove spyware and adware, you can obtain spyware and adware removers that can detect and delete spyware and adware. Some operating systems and Web browsers include spyware removers.

Privacy Laws

The concern about privacy has led to the enactment of federal and state laws regarding the storage and disclosure of personal data (Figure 11-36). Common points in some of these laws are outlined at the top of the next page.

1. Information collected and stored about individuals should be limited to what is necessary to carry out the function of the business or government agency collecting the data.
2. Once collected, provisions should be made to restrict access to the data to those employees within the organization who need access to it to perform their job duties.
3. Personal information should be released outside the organization collecting the data only when the person has agreed to its disclosure.
4. When information is collected about an individual, the individual should know that the data is being collected and have the opportunity to determine the accuracy of the data.

One law with an apparent legal loophole is the 1970 Fair Credit Reporting Act. The act limits the rights of others viewing a credit report to only those with a legitimate business need. The problem is that it does not define a legitimate business need. The result is that just about anyone can claim a legitimate business need and gain access to your credit report.
<table>
<thead>
<tr>
<th>Date</th>
<th>Law</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>Telephone Records and Privacy Protection Act</td>
<td>Makes it illegal to use fraudulent means to obtain someone’s telephone records.</td>
</tr>
<tr>
<td>2003</td>
<td>CAN-SPAM Act</td>
<td>Gives law enforcement the right to impose penalties on people using the Internet to distribute spam.</td>
</tr>
<tr>
<td>2002</td>
<td>Sarbanes-Oxley Act</td>
<td>Requires corporate officers, auditors, and attorneys of publicly-traded companies follow strict financial reporting guidelines.</td>
</tr>
<tr>
<td>2001</td>
<td>Children’s Internet Protection Act (CIPA)</td>
<td>Protects minors from inappropriate content when accessing the Internet in schools and libraries.</td>
</tr>
<tr>
<td>2001</td>
<td>Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act</td>
<td>Gives law enforcement the right to monitor people’s activities, including Web and e-mail habits.</td>
</tr>
<tr>
<td>1999</td>
<td>Gramm-Leach-Bliley Act (GLBA) or Financial Modernization Act</td>
<td>Protects consumers from disclosure of their personal financial information and requires institutions to alert customers of information disclosure policies.</td>
</tr>
<tr>
<td>1998</td>
<td>Children’s Online Privacy Protection Act (COPPA)</td>
<td>Requires Web sites protect personal information of children under 13 years of age.</td>
</tr>
<tr>
<td>1998</td>
<td>Digital Millennium Copyright Act (DMCA)</td>
<td>Makes it illegal to circumvent antipiracy schemes in commercial software; outlaws sale of devices that copy software illegally.</td>
</tr>
<tr>
<td>1997</td>
<td>No Electronic Theft (NET) Act</td>
<td>Closes a narrow loophole in the law that allowed people to give away copyrighted material (such as software) on the Internet without legal repercussions.</td>
</tr>
<tr>
<td>1996</td>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>Protects individuals against the wrongful disclosure of their health information.</td>
</tr>
<tr>
<td>1996</td>
<td>National Information Infrastructure Protection Act</td>
<td>Penalizes theft of information across state lines, threats against networks, and computer system trespassing.</td>
</tr>
<tr>
<td>1994</td>
<td>Computer Abuse Amendments Act</td>
<td>Amends 1984 act to outlaw transmission of harmful computer code such as viruses.</td>
</tr>
<tr>
<td>1992</td>
<td>Cable Act</td>
<td>Extends the privacy of the Cable Communications Policy Act of 1984 to include cellular and other wireless services.</td>
</tr>
<tr>
<td>1988</td>
<td>Computer Matching and Privacy Protection Act</td>
<td>Regulates the use of government data to determine the eligibility of individuals for federal benefits.</td>
</tr>
<tr>
<td>1988</td>
<td>Video Privacy Protection Act</td>
<td>Forbids retailers from releasing or selling video-rental records without customer consent or a court order.</td>
</tr>
<tr>
<td>1986</td>
<td>Electronic Communications Privacy Act (ECPA)</td>
<td>Provides the same right of privacy protection for the postal delivery service and telephone companies to the new forms of electronic communications, such as voice mail, e-mail, and cell phones.</td>
</tr>
<tr>
<td>1984</td>
<td>Cable Communications Policy Act</td>
<td>Regulates disclosure of cable television subscriber records.</td>
</tr>
<tr>
<td>1984</td>
<td>Computer Fraud and Abuse Act</td>
<td>Outlaws unauthorized access of federal government computers.</td>
</tr>
<tr>
<td>1978</td>
<td>Right to Financial Privacy Act</td>
<td>Strictly outlines procedures federal agencies must follow when looking at customer records in banks.</td>
</tr>
<tr>
<td>1974</td>
<td>Privacy Act</td>
<td>Forbids federal agencies from allowing information to be used for a reason other than that for which it was collected.</td>
</tr>
<tr>
<td>1974</td>
<td>Family Educational Rights and Privacy Act</td>
<td>Gives students and parents access to school records and limits disclosure of records to unauthorized parties.</td>
</tr>
<tr>
<td>1970</td>
<td>Fair Credit Reporting Act</td>
<td>Prohibits credit reporting agencies from releasing credit information to unauthorized people and allows consumers to review their own credit records.</td>
</tr>
</tbody>
</table>

Figure 11-36  Summary of the major U.S. government laws concerning privacy.
Social Engineering

As related to the use of computers, social engineering is defined as gaining unauthorized access or obtaining confidential information by taking advantage of the trusting human nature of some victims and the naivety of others. Some social engineers trick their victims into revealing confidential information such as user names and passwords on the telephone, in person, or on the Internet. Techniques they use include pretending to be an administrator or other authoritative figure, feigning an emergency situation, or impersonating an acquaintance. Social engineers also obtain information from users who do not destroy or conceal information properly. These perpetrators sift through company dumpsters, watch or film people dialing telephone numbers or using ATMs, and snoop around computers looking for openly displayed confidential information.

Employee Monitoring

Employee monitoring involves the use of computers to observe, record, and review an employee's use of a computer, including communications such as e-mail messages, keyboard activity (used to measure productivity), and Web sites visited. Many programs exist that easily allow employers to monitor employees. Further, it is legal for employers to use these programs.

A frequently debated issue is whether an employer has the right to read employee e-mail messages. Actual policies vary widely. Some companies declare that they will review e-mail messages regularly, and others state that e-mail messages are private. In some states, if a company does not have a formal e-mail policy, it can read e-mail messages without employee notification.

One survey discovered that more than 73 percent of companies search and/or read employee files, voice mail, e-mail messages, Web connections, and other networking communications. Several lawsuits have been filed against employers because many believe that such internal communications should be private. Read Ethics & Issues 11-5 for a related discussion.

Another controversial issue relates to the use of cameras to monitor employees, customers, and the public. Many people feel that this use of video cameras is a violation of privacy.

Content Filtering

One of the more controversial issues that surround the Internet is its widespread availability of objectionable material, such as racist literature, violence, and obscene pictures. Some believe that such materials should be banned. Others believe that the materials should be filtered, that is, restricted. Content filtering is the process of restricting access to certain material on the Web. Content filtering opponents argue that banning any materials violates constitutional guarantees of free speech and personal rights.

Many businesses use content filtering to limit employees’ Web access. These businesses argue that employees are unproductive when visiting inappropriate or objectionable Web sites. Some schools, libraries, and parents use content filtering to restrict access to minors.

One approach to content filtering is through a rating system of the Internet Content Rating Association (ICRA), which is similar to those used for movies and videos. Major Web sites such as

ETHICS & ISSUES 11-5

Should Text Messages Sent by Employees Be Private?

When an employee sends or receives an e-mail message using his or her employer’s e-mail server, the company most likely retains a backup of the message, which can be used as evidence against the employee if the employee is suspected of engaging in unscrupulous activity. When an employee sends a text message using a company-issued smart phone for such activity, however, the smart phone provider may store a record of the message. Even if an employer requires an employee to disclose all text message communications with customers, vendors, and competitors, the employee is not required legally to divulge those communications. If the employer accuses an employee of possibly violating only company policy, rather than a law, then the smart phone provider is not allowed to disclose the communications. While recent court rulings only confuse the issue further, the courts seem to side with employee privacy regarding the content of sent text messages. Employers argue, however, that because they provide the devices and service to the employee, they should have a right to view the content of the messages.

Should text messages sent by employees be private? Why or why not? How can employers create and enforce policies regarding the content of text messages sent on employer-issued smart phones? Should employers demand that smart phone providers offer the option to send all employee text message communications to the company on a monthly basis? Why or why not?
Yahoo!, AOL, and MSN use the rating system established by the ICRA. If content at the Web site goes beyond the rating limits set in the Web browser software, a user cannot access the Web site. Concerned parents can set the rating limits and prevent these limits from being changed by using a password.

Another approach to content filtering is to use filtering software. **Web filtering software** is a program that restricts access to specified Web sites. Some also filter sites that use specific words. Others allow you to filter e-mail messages, chat rooms, and programs. Many Internet security programs include a firewall, antivirus program, and filtering capabilities combined (Figure 11-37).

Since 2001, the federal government, local governments, businesses, and individuals have been implementing aggressive new security measures because of the increase in terrorist activity. A security threat can exist anywhere, and it is nearly impossible for humans alone to protect the country. As a result, computers now assist governments, law enforcement officials, business owners, and other individuals with monitoring and maintaining security.

Advancements in computer vision enable computers to monitor indoor and outdoor areas that might be subject to a high amount of criminal activity. For example, some cities are installing cameras in problematic areas. A computer program analyzes the output from the camera and can determine whether two or more people in close proximity to one another might be engaged in a physical confrontation. If the computer detects suspicious behavior, it automatically notifies local law enforcement.

Computers also use facial recognition to identify individuals who do not belong in a particular area. For example, one theme park in Florida often takes a picture of individuals they escort out of and ban from the park. As visitors walk from their cars to the park, surveillance cameras positioned in strategic locations scan visitors’ faces and compare them to the database containing images of those who are banned from the park. If the computer finds a match, it alerts a security officer who then can investigate the situation. Thousands of people visit theme parks each day, and computers make it easier to perform the otherwise impossible task of identifying those who might be trespassing.

The federal government, particularly the Department of Homeland Security, uses a computerized No Fly List to track individuals who are not authorized to travel on commercial flights within the United States. When an individual makes a reservation, a computer compares his or her name to the database containing images of those who are banned from the park. If the computer finds a match, it alerts a security officer who then can investigate the situation. Thousands of people visit theme parks each day, and computers make it easier to perform the otherwise impossible task of identifying those who might be trespassing.

Whether you are walking outside, visiting an attraction, or traveling, the chances are good that computers are, in some way, ensuring your safety.

For more information, visit scsite.com/dc2011/ch11/ work and then click National and Local Security.

**File:** 11-37

Many Internet security programs include content filtering capabilities, where users can block specified Web sites and applications.
As mentioned in this chapter, encryption is a process of converting readable data into unreadable characters to prevent unauthorized access. Various encryption algorithms are used to encrypt data, with some more secure than others. The chapter showed a few simple encryption algorithms. Individuals and organizations often desire more secure encryption, which requires a complex encryption algorithm. Thousands of encryption algorithms exist, and it is even possible to write your own. Commonly used secure encryption algorithms include Blowfish, DES, 3DES, and IDEA.

The Blowfish encryption algorithm was introduced in 1993 as a free alternative to other encryption algorithms that were available at that time. Blowfish, which has been thoroughly tested since its development and has proven to be a strong algorithm, uses a key length varying between 32 and 448 bits and is applied to a block of data as opposed to single bits of data.

The DES (Data Encryption Standard) encryption algorithm in the late 1970s was developed by the United States government and IBM. This standard uses a 56-bit key to encrypt 64-bit blocks of data at a time. The encryption process requires that each block of the message go through 16 different stages, adding to the strength of the algorithm. Advancements in technology, however, made it easier and faster for computers with increased processing capabilities to decrypt these 56-bit keys, which were only 7 characters long. As a result, the Triple-DES (3DES) encryption algorithm was developed. This algorithm uses the original Data Encryption Standard to encrypt the data with the first 56-bit key and then decrypts the data with another 56-bit key. Finally, a third 56-bit key encrypts the data once again. This process creates a total key length of 168 bits, which is significantly more difficult to compromise.

IDEA (International Data Encryption Algorithm) was developed in the early 1990s to replace the DES encryption algorithm. This algorithm uses the same key for encryption and decryption on blocks of data that are 64 bits long. Unlike the DES algorithm, IDEA uses a 128-bit key, greatly increasing the complexity and security of the encrypted data.

The U.S. government uses the Advanced Encryption Standard (AES), mostly for unclassified data. In addition, various other organizations use AES. Windows 7 Ultimate edition includes BitLocker Drive Encryption (Figure 11-38), a security feature using the Encrypting File System (EFS) to encrypt data. EFS uses the Advanced Encryption Standard to protect files and data from almost any method of unauthorized access. When a user encrypts a file, EFS generates a random number for the file that EFS calls the file’s FEK (file encryption key) to encrypt the data. EFS then uses FEK to encrypt the file’s contents with the encryption algorithm. The user’s public key then encrypts the FEK using the RSA public-key-based encryption algorithm, and the encrypted FEK then is stored with the file. The entire encryption process happens behind the scenes for the user, who simply completes a few mouse clicks to encrypt a folder or file. That is part of the elegance of EFS: while it is simple for a user, it is very difficult for any unauthorized user without the correct keys to crack the encryption. In the end, that is the key to keeping your data safe and sound.

For more information, visit scsite.com/dc2011/ch11/tech and then click Encryption Algorithms.

Figure 11-38 One authentication scenario in BitLocker Drive Encryption.
Symantec’s programmers analyzed every line of code, rewrote programs, and developed a new security model to create its latest versions of Norton AntiVirus and Norton Internet Security. The results are programs that use less hard disk space, decrease starting and scanning time, and average less than 7 MB of memory. The more than 100 performance improvements offer advanced protection for millions of computer users worldwide.

The California-based company is one of the ten largest software corporations in the world. It was founded in 1982 and has offices in more than 40 countries. Its primary manufacturing facility is located in Dublin, Ireland. In 2009, Symantec released the latest version of its Norton Internet Security software. A rating service tested the level of protection provided by 10 different security products and gave Norton Internet Security the only perfect score.

The McAfee Initiative to Fight Cybercrime is a global effort to thwart security threats and criminal activity. The world’s largest dedicated security technology company has partnered with experts in law enforcement, education, government, and society to investigate, prosecute, and attempt to prevent security breaches.

McAfee products protect more than 60 million consumers, small- and medium-sized businesses, governmental agencies, and large corporations from malware, spam, and unauthorized access. In addition, more than 100 million mobile devices are protected with McAfee software. The corporation takes its name from its founder, John McAfee, who started the company in 1987 from his Santa Clara, California, home.

In 2009, McAfee launched a new online backup service with unlimited capacity that allows consumers to back up and encrypt their important files such as documents, photos, music, and e-mail messages.

For more information, visit scsite.com/dc2011/ch11/companies.

RICHARD STALLMAN Software Freedom Advocate

Stallman began the GNU/Linux Project in 1983 as an effort to develop and use the copyleft concept. Linux is an outgrowth of this project, which continues to be a forum for software development, ethical practices, and political campaigning. He also started the Free Software Foundation (FSF) in 1985 to promote writing free software for the GNU Project. The Free Software Directory catalogs more than 5,300 packages that run on the Linux and GNU operating systems.

For 30 years, he has advised major corporations, including Microsoft, Intel, and Unisys, the U.S. Air Force, the Federal Bureau of Investigation, and two U.S. presidents. He is noted for several firsts in the computer security field. For example, he defined the terms, software forensics and firewall, wrote the first English-language book on the topics of viruses and malware, and founded the world’s first multidisciplinary academic security awareness group: the Center for Education and Research in Information Assurance and Security (CERIAS).

For more information, visit scsite.com/dc2011/ch11/trailblazers.
Chapter Review

The Chapter Review reinforces the main concepts presented in this chapter.

1. **What Are Computer Security Risks, and What Are the Types of Cybercrime Perpetrators?** A computer security risk is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability. Any illegal act involving a computer is a computer crime; the term cybercrime refers to online or Internet-based illegal acts. Perpetrators of cybercrime include: hacker, cracker, script kiddie, corporate spy, unethical employee, cyberextortionist, and cyberterrorist.

2. **What Are Various Internet and Network Attacks, and How Can Users Safeguard against These Attacks?** A computer virus is a potentially damaging program that affects, or infects, a computer negatively by altering the way the computer works without the user's knowledge or permission. A worm is a program that copies itself repeatedly, using up resources and possibly shutting down the computer or network. A Trojan horse is a program that hides within or looks like a legitimate program. A rootkit is a program that hides in a computer and allows someone from a remote location to take full control of the computer. To take precautions against this malware, do not start a computer with removable media in the drives or ports. Never open an e-mail attachment unless you are expecting the attachment and it is from a trusted source. Disable macros in documents that are not from a trusted source. Install an antivirus program and a personal firewall. Stay informed about any new virus alert or virus hoax. To defend against a botnet, a denial of service attack, improper use of a back door, and spoofing, users can install a firewall, install intrusion detection software, and set up a honeypot. To obtain help from other students about any concept in this chapter, visit scsite.com/dc2011/ch11/forum and post your thoughts and questions.

3. **What Are Techniques to Prevent Unauthorized Computer Access and Use?** Unauthorized access is the use of a computer or network without permission. Unauthorized use is the use of a computer or its data for unapproved or illegal activities. Organizations can take measures such as implementing a written acceptable use policy (AUP), a firewall, intrusion detection software, an access control, and an audit trail. Access controls include a user name and password or passphrase, a CAPTCHA, a possessed object, and a biometric device.

4. **What Are Safeguards against Hardware Theft and Vandalism?** Hardware theft is the act of stealing computer equipment. Hardware vandalism is the act of defacing or destroying computer equipment. The best preventive measures against hardware theft and vandalism are common sense and a constant awareness of the risk. Physical devices and practical security measures, such as locked doors and windows, can help protect equipment. Passwords, possessed objects, and biometrics can reduce the risk of theft or render a computer useless if it is stolen.

5. **How Do Software Manufacturers Protect against Software Piracy?** Software piracy is the unauthorized and illegal duplication of copyrighted software. To protect themselves from software piracy, manufacturers issue a license agreement and require product activation.

6. **How Does Encryption Work, and Why Is It Necessary?** Encryption prevents information theft and unauthorized access by converting readable data into unreadable characters. To read the data, a recipient must decrypt, or decipher, it into a readable form. An encryption algorithm, or cipher, converts readable plaintext into unreadable ciphertext. Encryption is used to protect information on the Internet and networks.

7. **What Types of Devices Are Available to Protect Computers from System Failure?** A system failure is the prolonged malfunction of a computer. A common cause of system failure is an electrical power variation such as noise, undervoltage, or an overvoltage. A surge protector, also called a surge suppressor, uses special electrical components to smooth out minor noise, provide a stable current flow, and keep an overvoltage from reaching the computer and other electronic equipment.
An uninterruptible power supply (UPS) contains surge protection circuits and one or more batteries that can provide power during a temporary loss of power.

8. What Are Options for Backing Up Computer Resources? A backup is a duplicate of a file, program, or disk that can be used to restore the file if the original is lost, damaged, or destroyed. Users can opt for a full backup or a selective backup. Some users implement a three-generation backup policy that preserves three copies of important files: the grandparent, the parent, and the child. Others use RAID or continuous backup. Most operating systems and backup devices include a backup program.

9. What Risks and Safeguards Are Associated with Wireless Communications? Wireless access poses additional security risks. Intruders connect to other wireless networks to gain free Internet access or an organization’s confidential data. Some individuals intercept and monitor communications as they transmit. Others connect to a network through an unsecured wireless access point (WAP), sometimes using the techniques of war driving or war flying. Some safeguards include firewalls, reconfiguring the WAP, and ensuring equipment uses a wireless security standard, such as Wi-Fi Protected Access (WPA) and 802.11i.

10. How Can Health-Related Disorders and Injuries Due to Computer Use Be Prevented? A computer-related repetitive strain injury (RSI) can include tendonitis and carpal tunnel syndrome (CTS). Another health-related condition is eyestrain associated with computer vision syndrome (CVS). To prevent health-related disorders, take frequent breaks, use precautionary exercises and techniques, and use ergonomics when planning the workplace. Computer addiction occurs when the computer consumes someone’s entire social life.

11. What Are Issues Related to Information Accuracy, Intellectual Property Rights, Codes of Conduct, and Green Computing? Computer ethics govern the use of computers and information systems. Issues in computer ethics include the responsibility for information accuracy and the intellectual property rights to which creators are entitled for their works. An IT (information technology) code of conduct helps determine whether a specific computer action is ethical or unethical. Green computing reduces the electricity and environmental waste while using a computer.

12. What Are Issues Surrounding Information Privacy? Information privacy is the right of individuals and companies to deny or restrict the collection and use of information about them. Issues surrounding information privacy include the following. An electronic profile combines data about an individual’s Web use with data from public sources, which then is sold. A cookie is a file that a Web server stores on a computer to collect data about the user. Spyware is a program placed on a computer that secretly collects information about the user. Adware is a program that displays an online advertisement in a banner or pop-up window. Spam is an unsolicited e-mail message or newsgroup posting sent to many recipients or newsgroups at once. Phishing is a scam in which a perpetrator attempts to obtain personal or financial information. The concern about privacy has led to the enactment of many federal and state laws regarding the disclosure of data. As related to the use of computers, social engineering is defined as gaining unauthorized access or obtaining confidential information by taking advantage of the trusting human nature of some victims and the naivety of others. Employee monitoring uses computers to observe, record, and review an employee’s computer use. Content filtering restricts access to certain materials on the Web.
### Key Terms

You should know the Primary Terms and be familiar with the Secondary Terms. The list below helps focus your study.

To see an example of and a definition for each term, and to access current and additional information from the Web, visit scsite.com/dc2011/ch11/terms.

#### Primary Terms

- anti-spam program (587)
- antivirus program (560)
- audit trail (565)
- back door (562)
- back up (577)
- backup (577)
- biometric device (568)
- botnet (562)
- code of conduct (582)
- computer crime (556)
- computer ethics (581)
- computer security risk (556)
- computer vision syndrome (579)
- content filtering (590)
- cookie (585)
- copyright (582)
- cracker (556)
- cybercrime (556)
- cyberextortionist (557)
- cyberterrorist (557)
- decrypt (573)
- denial of service attack (562)
- digital certificate (574)
- digital forensics (569)
- digital signature (574)
- DoS attack (562)
- e-mail filtering (587)
- employee monitoring (590)
- encryption (573)
- Fair Credit Reporting Act (588)
- firewall (563)
- hacker (556)
- hardware theft (570)
- hardware vandalism (570)
- information privacy (584)
- information theft (572)
- inoculate (561)
- intellectual property rights (582)
- license agreement (571)
- noise (575)
- online service security (558)
- overvoltage (575)
- password (566)
- personal firewall (564)
- personal identification number (PIN) (568)
- phishing (587)
- piracy (571)
- power surge (575)
- product activation (572)
- quarantine (561)
- repetitive strain injury (RSI) (579)
- restore (577)
- rootkit (558)
- script kiddie (556)
- secure site (574)
- social engineering (590)
- software theft (571)
- spam (587)
- spoofing (563)
- surge protector (576)
- Trojan horse (558)
- trusted source (560)
- unauthorized access (564)
-未经授权的use (564)
- undervoltage (575)
- uninterruptible power supply (UPS) (576)
- user name (566)
- virus (558)
- virus definition (560)
- virus hoax (561)
- virus signature (560)
- Web filtering software (591)
- worm (558)
- zombie (562)

#### Secondary Terms

- 1024-bit encryption (574)
- 128-bit encryption (574)
- 40-bit encryption (574)
- 802.11i (573)
- access control (565)
- access point mapping (578)
- adware (588)
- asymmetric key encryption (573)
- authentication (585)
- biometric payment (568)
- blackout (575)
- bot (562)
- breach (575)
- Business Software Alliance (BSA) (572)
- CAPTCHA (567)
- carpal tunnel syndrome (CTS) (579)
- CERT/CC (558)
- certificate authority (CA) (574)
- child (577)
- cyberextortionist (557)
- clickjacking (588)
- computer Emergency Response Team Coordination Center (558)
- computer forensics (569)
- crimeware (556)
- CVSS (579)
- cyberforensics (569)
- cyberwarfare (557)
- cyberwire (557)
- ciphers (572)
- DDoS (distributed DoS) attack (562)
- digital right management (DRM) (582)
- email spoofing (563)
- encryption algorithm (573)
- encryption key (573)
- end-user license agreement (EULA) (571)
- ENERGY STAR program (583)
- ergonomics (580)
- fault-tolerant computer (577)
- full backup (577)
- grandfather (577)
- backup (574)
- honeypot (564)
- identification (565)
- intellectual property (IP) (582)
- Internet Content Rating Association (ICRA) (590)
- intrusion detection software (564)
- IP spoofing (563)
- journey (576)
- keygen (571)
- macro (560)
- malicious software (558)
- malware (558)
- network forensics (569)
- offline UPS (576)
- offline UPS (577)
- online UPS (577)
- parent (577)
- passphrase (566)
- payload (558)
- phishing filter (587)
- plaintext (573)
- possessed object (568)
- power usage effectiveness (583)
- Pretty Good Privacy (PGP) (574)
- private key encryption (573)
- proxy server (564)
- public key encryption (573)
- real-time location system (RTLS) (570)
- Secure HTTP (S-HTTP) (573)
- Secure Socket Layer (SSL) (575)
- select backup (577)
- session cookie (586)
- single-user license agreement (571)
- spike (573)
- spin (587)
- spyware (558)
- SSD (578)
- standby UPS (576)
- surge suppressor (556)
- symmetric key encryption (573)
- system failure (575)
- tendonitis (579)
- three-generation backup (577)
- Transport Layer Security (TLS) (575)
- Underwriters Laboratories (UL) (575)
- 1449 standard (576)
- user ID (566)
- virtual private network (VPN) (575)
- war driving (578)
- war flying (578)
- Web bug (588)
- Wi-Fi Protected Access (WPA) (578)
- zombie army (562)

---

**Surge protector (576)**
Checkpoint

The Checkpoint exercises test your knowledge of the chapter concepts. The page number containing the answer appears in parentheses after each exercise. The Beyond the Book exercises will help broaden your understanding of the concepts presented in this chapter.

To complete the Checkpoint exercises interactively, visit scsite.com/dc2011/ch11/check.

True/False  Mark T for True and F for False.

____ 1. Not all breaches to computer security are planned. (556)
____ 2. The term, cyberwarfare, describes an attack whose goal ranges from disabling a government’s computer network to crippling a country. (557)
____ 3. Many methods exist to guarantee completely a computer or network is safe from computer viruses and other malware. (560)
____ 4. Cybervillains install malicious bots on unprotected computers to create a zombie army. (562)
____ 5. A honeypot is a computer that is isolated and, therefore, immune to attack. (564)
____ 6. Biometric payment involves a customer’s fingerprint being read by a fingerprint reader that is linked to a payment method such as a checking account or credit card. (568)
____ 7. Some businesses use a real-time location system (RTLS) to track and identify the location of high-risk or high-value items. (570)
____ 8. A program called a keygen, short for key generator, creates software registration numbers and sometimes activation codes. (571)
____ 9. With public key encryption, both the originator and the recipient use the same secret key to encrypt and decrypt the data. (573)
____ 10. A digital signature is a mathematical formula that generates a code from the contents of the message. (574)
____ 11. Digital rights management (DRM) is a strategy designed to prevent illegal distribution of movies, music, and other digital content. (582)
____ 12. Green computing involves reducing the electricity while using a computer, but the practice increases environmental waste. (583)

Multiple Choice  Select the best answer.

1. A _____ is a program that hides in a computer and allows someone from a remote location to take full control of the computer. (558)
   a. worm  b. rootkit  c. payload  d. cookie
2. Malware is a term that can be used to describe _____. (558)
   a. worms  b. rootkits  c. back doors  d. all of the above
3. A _____ is an assault whose purpose is to disrupt computer access to an Internet service such as the Web or e-mail. (562)
   a. denial of service attack  b. zombie  c. Trojan horse  d. virus hoax
4. _____ involves the examination of computer media, programs, data and log files on computers, servers, and networks. (569)
   a. Encryption key  b. E-mail filtering  c. Digital forensics  d. Trusted source
5. Physical access controls, such as locked doors and windows, usually are adequate to protect against _____. (570)
   a. software piracy  b. unauthorized access  c. hardware theft  d. all of the above
6. A(n) _____ is a programmed formula that the originator of the data uses to encrypt the plaintext and the recipient of the data uses to decrypt the ciphertext. (573)
   a. botnet  b. certificate authority  c. encryption algorithm  d. encryption key
7. Some organizations continually review their _____, which is a ratio that measures how much power enters the computer facility, or data center, against the amount of power required to run the computers. (583)
   a. uninterruptible power supplies  b. public key encryption  c. ENERGY STAR program  d. power usage effectiveness (PUE)
8. As related to the use of computers, _____ is defined as gaining unauthorized access or obtaining confidential information by taking advantage of the trusting human nature of some victims and the naivety of others. (590)
   a. phishing  b. pharming  c. social engineering  d. a virus hoax
Checkpoint

Matching  Match the terms with their definitions.

1. virus (558) a. set of steps that can convert readable plaintext into unreadable ciphertext
2. trusted source (560) b. private combination of words, often containing mixed capitalization and punctuation, associated with a user name that allows access to certain computer resources
3. quarantine (561) c. protects a personal computer and its data from unauthorized intrusions
4. botnet (562) d. organization or person you believe will not send a virus infected file knowingly
5. spoofing (563) e. area of the hard disk that holds an infected file until the infection can be removed
6. personal firewall (564) f. uses special electrical components to smooth out minor noise, provide a stable current flow, and keep an overvoltage from reaching the computer and other electronic equipment
7. passphrase (566) g. group of compromised computers connected to a network such as the Internet that is being used as part of a network that attacks other networks, usually for nefarious purposes
8. encryption algorithm (573) h. translates a personal characteristic into digital code
9. biometric device (568) i. technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network
10. surge protector (576) j. potentially damaging computer program that affects, or infects, a computer negatively by altering the way the computer works without the user’s knowledge or permission

Short Answer  Write a brief answer to each of the following questions.

1. How do antivirus programs detect and identify a virus? ____________________________ What is a virus hoax? ____________________________
2. Describe the ENERGY STAR program. ____________________________ How should users handle obsolete computers? ____________________________
3. What is information privacy? ____________________________ List five ways to safeguard your personal information. ____________________________
4. What are two methods for avoiding phishing attacks? ____________________________ How does clickjacking work? ____________________________
5. Who uses content filtering and why? ____________________________ Describe a rating system used for content filtering. ____________________________

Beyond the Book  Follow the book element instructions below; present your findings (brief report, presentation, discussion, or other means).

1. Ethics & Issues — Select an Ethics & Issues in this chapter (562, 568, 572, 588, 590), find a recent newspaper/magazine article that supports one point of view presented, and then evaluate the article.
2. Computer Usage @ Work — Use the Web or a recent newspaper/magazine to locate three additional unique usages of computer technology in the national and local security field (591). What makes the use of these technologies unique to the national and local security field?
3. Companies on the Cutting Edge and Technology Trailblazers — Use the Web or a recent newspaper/magazine to locate an interesting fact about McAfee, Symantec, Richard Stallman, or Gene Spafford that was not presented in the chapter (593).
4. High-Tech Talk — Locate a recent newspaper/magazine article that discusses topics related to Encryption Algorithms (592). Would you recommend the article you found? Why or why not?
5. FAQs and Web Links — Use the Web or a recent newspaper/magazine to locate three additional facts about an FAQ (559, 562, 567, 569, 577, 578, 587, 588) and Web Link (538, 562, 564, 568, 570, 572, 574, 576, 578, 582, 586, 590) that were not presented in the chapter.
6. Looking Ahead — Use the Web or a recent newspaper/magazine to discover additional uses of the technology presented in Brain Waves, Behavior Tracked to Prevent and Solve Crimes (569).
7. Innovative Computing — Use the Web or a recent newspaper/magazine to locate two additional interesting facts about RECAPTCHA Help Digitize Newspapers, Books (567) or Customers’ Behavior, Conversations Monitored (585).
8. Making Use of the Web — Visit three of the Learning sites (135) and outline the information on each Web site and the possible uses for each Web site.
9. Digital Forensics — Select a topic from the Digital Forensics feature (606) and then create a presentation about the topic using the Web or a magazine article. Discuss how the tools and techniques in the feature were used to solve a real crime.
Learn It Online

The Learn It Online exercises are interactive Web exercises designed to reinforce and expand your understanding of the chapter concepts. The descriptions below briefly summarize each exercise.

To access the Learn It Online exercises and for specific exercise instructions, visit scsite.com/dc2011/ch11/learn.

1. **At the Movies — Attack of the Mobile Viruses**
   Watch a movie to learn about the recent wave of viruses plaguing mobile device users and then answer questions about the movie.

2. **Video and Audio: You Review It — Green Computing**
   Search for, choose, and write a review of a video, podcast, or vodcast that discusses green computing.

3. **Student Edition Labs — Protecting Your Privacy Online and Computer Ethics**
   Enhance your understanding and knowledge about online privacy and computer ethics by completing the Protecting Your Privacy Online and Computer Ethics Labs.

4. **Practice Test**
   Take a multiple choice test that checks your knowledge of the chapter concepts and review the resulting study guide.

5. **Who Wants To be a Computer Genius2?**
   Play the Shelly Cashman Series version of this popular game by answering questions to find out if you are a computer genius. Panic buttons are available to provide assistance during game play.

6. **Wheel of Terms**
   Identify important key terms presented in this chapter by playing the Shelly Cashman Series version of this popular game.

7. **DC Track and Field**
   Practice or compete against other students in three track and field events by answering multiple choice, true/false, and short answer questions related to concepts discussed in this chapter.

8. **You’re Hired!**
   Embark on the path to a career in computers by answering questions and solving puzzles related to concepts discussed in this chapter.

9. **Crossword Puzzle Challenge**
   Complete an interactive crossword puzzle to reinforce concepts presented in this chapter.

10. **Windows Exercises**
    Step through the Windows 7 exercises to learn about playing audio compact discs, understanding multimedia properties, dragging and dropping Windows objects, and checking for system updates.

11. **Exploring Computer Careers**
    Read about a career as a digital forensics examiner, search for related employment advertisements, and then answer related questions.

12. **Web Apps — Dictionary.com**
    Learn how to use Dictionary.com to search for a dictionary entry, translate a word to other languages, and search for Web pages containing your search term.
Problem Solving @ Home

The Problem Solving @ Home exercises extend your knowledge of the chapter concepts by seeking solutions to practical computer problems that you may encounter at home or school. The Collaboration exercise should be completed with a team.

To discuss the Problem Solving @ Home exercises with other students, visit scsite.com/dc2011/ch11/forum and post your thoughts or questions.

1. Infected File Detected A message appears on your computer screen stating that your antivirus program detected an infected file on your computer and is unable to move it to quarantine. What are your next steps?

2. Unsolicited E-Mail Attachment You have opened an e-mail message from your best friend stating that he has attached a photo from his recent Caribbean vacation. You are unaware that your friend had taken a vacation, but you attempt to open the photo anyway. After double-clicking the attachment, the photo does not open. You immediately call your friend to ask for help, and he informs you that he did not send that e-mail message to you. What might have happened?

3. Product Key in Use While installing the latest version of Microsoft Office, the installation program prompts you to enter the product key. Once you finish entering the product key, you receive an error message stating that the product key already is in use. What might be causing this?

4. Questionable Fair Use A media company’s attorney has sent you a letter stating that you are violating their rights by including a short movie clip from one of their movies in one of your videos posted on YouTube. You believe that you are within fair use guidelines by including the movie clip but also feel that you should respond to the attorney’s letter. What are your next steps?

5. Shutting Down Safely While working on your computer, the power suddenly fails. Luckily, your computer is connected to a UPS and you are able to continue working; however, you are not certain how much time you have before the UPS battery runs out. What steps will you take to shut down your computer safely without losing data?

6. Unauthorized Computer on Network You are viewing the configuration for your wireless router, as well as the computers that are connected to your wireless network. In addition to the two desktop computers and one notebook computer in your house, you notice that another computer is connected to your wireless network. How could this be?

7. Verifying Photo Validity You are writing a research paper for your history class and have found a photo on the Web that you would like to use. You are cautious about using photos on the Web because of copyright issues and photos that have been altered digitally. How might you verify the validity of a photo on the Web?

Collaboration

8. Minimizing Computer Threats Because you have just started college, your parents purchased a new computer for you. You wish to protect it as much as possible from threats such as power surges and power outages, unauthorized use and vandalism, and hard disk failure. Form a team of three classmates who will research how to minimize potential threats. One team member should research ways to safeguard your computer from power surges, power outages, and other electrical variations. Another team member will research ways to safeguard your computer from unauthorized use and vandalism, and the third team member will research two backup strategies that will be used to store important backups in the event of a hard disk failure. The three team members should locate and suggest products that will help to safeguard your new computer, discuss their findings, compile them into a brief report, and then submit it to the instructor.
Problem Solving @ Work

The Problem Solving @ Work exercises extend your knowledge of the chapter concepts by seeking solutions to practical computer problems that you may encounter at work. The Collaboration exercise should be completed with a team.

To discuss the Problem Solving @ Work exercises with other students, visit scsite.com/dc2011/ch11/forum and post your thoughts or questions.

In the real world, practical problems often can be solved in multiple ways. Provide one solution to each of the following problems using available resources, such as articles on the Web or in print, blogs, podcasts, videos, television, user guides, other individuals, and electronics and computer stores. You may need to use multiple resources to obtain an answer. Present your solutions in the form requested by your instructor (brief report, presentation, discussion, or other means).

1. Unknown Computer User  When you arrive to work each day, you frequently notice that your keyboard and mouse have been moved from the location you left it in the previous day. In addition, your Web browser’s history lists sites that you have not visited. You suspect that someone uses your computer while you are out of the office. What are some ways to prevent this?

2. Forgot Decryption Password  To safeguard some of your important files from others, you decide to encrypt them. Upon attempting to decrypt the files so that you can access them, however, you are unable to remember the correct password. What are your next steps?

3. Password Management  You must remember multiple user names and passwords to access various computer resources within your company. Each time your company introduces a new system, you must remember a new user name and password, some of which you are unable to customize. What steps will you take to manage your passwords?

4. Problem Reinstalling Software  After recovering from a computer crash, you attempt to reinstall a program that was previously installed. When you insert the installation media, begin the installation, and type the product key, you receive an indication that you are unable to continue installing the software because you have installed it the maximum number of allowable times. What are your next steps?

5. Surge Protector Malfunctioning  While picking up a dropped item from the floor, you notice that the lights on your surge protector are not illuminated. All the devices plugged into the surge protector appear to be functioning without issue, but you are curious as to why the lights are off. What might be wrong?

6. Missing Security Cable Key  To protect your notebook computer from theft, you use a security cable to secure it to the desk in your cubicle. Your boss assigns you some work to take home and suggests that you take home your notebook computer. You discover, however, that you are unable to locate the key that releases the security cable from the computer. What are your next steps?

7. Setting Up an Ergonomic Environment  After moving to a new office building, your company takes the opportunity to suggest that everyone set up an ergonomic working environment in their new office. What are some ways that you can set up an ergonomic work environment in your office?

8. Monitored Computer Activities  You receive an e-mail message from the IT department stating that it randomly will monitor employee computers throughout the workday to ensure that they are being used for legitimate purposes. Shortly thereafter, you begin to notice that your computer slows significantly at random times once or twice per week. You suspect the performance decrease is a result of the computer monitoring. How will you address this?

Collaboration

9. Computers in National and Local Security  National and local security agencies often use computers to protect citizens. For example, computers are used to maintain a list of individuals not cleared to board a commercial aircraft. Form a team of three people to create a list of the various ways computers help to keep us safe. One team member should research how local agencies, such as police departments, use computers to ensure security. Another team member should research ways national security agencies use computers to protect us from threats, and the last team member should research ways that private businesses use computers to guarantee security. Compile these findings into a report and submit it to your instructor.
Learn How To

The Learn How To activities step you through fundamental technology skills when using a computer. The Learn How To exercises enable you to become more proficient with these skills.

Premium Activity: To relate this Learn How To activity to your everyday life, see a visual demonstration of the activity, and then complete a short assessment, visit scsite.com/dc2011/ch11/howto.

Learn How To 1: Back Up Files on an Offsite Internet Server

Note: The service described in this exercise allows 15 days of free access. After that time, you may be billed automatically for service unless you cancel your service in the given time frame.

Back up files stored on your computer on another disk or computer located in a different geographical location is the ultimate safeguard for data on your computer. A good way to back up data is to use one of the services available on the Web. A leading service is found at IBackup.com.

To subscribe to the IBackup service, complete the following steps:

1. Start a Web browser, type the Web address IBackup.com in the Address bar and then press the Enter key.
2. When the IBackup Web page is displayed, click Signup on the top horizontal toolbar.
3. Enter your e-mail address in the E-mail Address text box and then click the Continue with Registration button to display a form (Figure 11-39).
4. Fill in the form. Select the plan you want in the Select a Storage Plan list. If you want to try the service for a short period of time before subscribing, select 5 GB 15 day Free Trial Plan.
5. To continue, you must enter credit card information. If you select the 15-day trial, your credit card will not be charged at this time, and an automatic billing at the end of 15 days will occur. After entering the required information, click the Continue button at the bottom of the page.
6. A message is displayed that confirms that you have signed up with IBackup and also provides a link for you to download the IBackup for Windows program.
7. Click the DOWNLOAD button to download the IBackup for Windows program and then follow the instructions to install the program on your computer.

After establishing an account, you can use it for the time for which you subscribed. Complete the following steps to use the service:

1. Start the IBackup for Windows program.
2. Enter your user name and password and then click the Connect button to open a window containing your files, as well as the contents of your My IBackup folder (Figure 11-40).
3. To upload a file, locate the file in the left pane of the IBackup window and drag it to the right pane. The Backup Progress dialog box will be displayed while the file is uploading. The file will be placed in the My IBackup folder.
4. For further activities you can accomplish in this program for backing up your files, click the buttons on the top horizontal toolbar and experiment.
Learn How To

Exercises

1. Visit the IBackup Web site. Click View Demo and then follow the screen prompts to view all the services offered by IBackup. Which service is most appropriate for your home computer? Which service is most useful for the server that is used in the computer lab at your school? If you had critical data you needed to back up, would you use a service like this? Why or why not? Submit your answers to your instructor.

2. Optional: Perform this exercise only for your own computer. Do not perform this exercise on a school computer. Establish an account on IBackup.com. Upload two or more files from your computer. Download the files you uploaded back to your computer. Is this an efficient way to back up your files? Do you think the IBackup service would be useful for businesses? Submit your answers to your instructor.

Learn How To 2: Use the Windows Firewall

When you use the Internet, data is sent both from your computer to the Internet and from computers on the Internet to your computer. A firewall is a barrier that checks information coming from the Internet and either turns it away or allows it to pass through to your computer, based on your firewall settings. It also checks data being sent from your computer to the Internet to ensure your computer is not sending unsolicited messages to other computers on the Internet. A firewall can be implemented using hardware or software.

Windows contains a software firewall that starts automatically when you boot your computer. To control the firewall usage on your computer, complete the following steps:

1. Click the Start button on the Windows taskbar and then click Control Panel on the Start menu.
2. Click the System and Security link and then click Windows Firewall in the System and Security window to open the Windows Firewall window (Figure 11-41).
3. Click the Allow a program or feature through Windows Firewall link to open the Allowed Programs window (Figure 11-42). The programs and features that are checked can communicate with the Internet without your clicking a link.
4. You may want to allow programs and features that routinely communicate with the Internet, such as sports programs that display updated game scores, to have full access to your computer. To add a program to the ‘Allowed programs and features’ list, click the ‘Allow another program’ button. The Add a Program dialog box is displayed. Select a program and then click the Add button.

Exercise

1. Open the Windows Firewall window. Click the ‘How does a firewall help protect my computer?’ link. Read the information about Windows Firewall. What did you learn that you did not know? What is malicious software? What are some examples of malicious software? Submit your answers to your instructor.
The Web Research exercises broaden your understanding of the chapter concepts by presenting questions that require you to search the Web for answers.

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search Sleuth</strong></td>
<td>Use one of the search engines listed in Figure 2-10 in Chapter 2 on page 85 or your own favorite search engine to find the answers to the following questions. Copy and paste the Web address from the Web page where you found the answer. Some questions may have more than one answer. If required, submit your answers to your instructor. (1) Which five words are among the most commonly used passwords? (2) What do e-mail messages with the subject lines “Sending You All My Love,” “Laughing Kitty,” and “You’ve Received a Postcard from a Family Member” have in common? (3) T’ai chi, yoga, and the Alexander technique might offer some relief to computer users suffering from which injury? (4) For which purpose is a gas discharge arrestor used? (5) How many computers in the business world have antivirus software that has been disabled or never was installed properly?</td>
</tr>
<tr>
<td><strong>Green Computing</strong></td>
<td>The more than 1 billion computers in the world each emit an average of 1,000 pounds of carbon dioxide each year. Many home computer users can help reduce their carbon footprint with the help of devices that monitor energy consumption. Computers are not the only home devices that draw a lot of current; the average home has 27 products that always are turned on, including the television, appliances, and heating and cooling systems. Verdiem’s free download, Edison, helps consumers manage their computer power usage. Smart metering devices made by Control4, Colorado vNet, and ZigBee track power usage and give automated tips on how to reduce energy costs. View online Web sites that provide information about reducing home electricity consumption. How do the monitoring devices work? How much do they cost? How do they calculate the money and energy saved per year? Write a report summarizing your findings, and include a table of links to Web sites that provide additional details.</td>
</tr>
<tr>
<td><strong>Social Networking</strong></td>
<td>People with unique and special talents often desire to share their passions and pastimes with others. Online social networks provide them an opportunity to share their hobbies and creations. In fact, 69 percent of online social networking members say they have a connection with special-interest Web sites. For example, members of the Sports MatchMaker (sportsmatchmaker.com) community can find people who want to play any sport or participate in any hobby at a specific date and time. ShowOffDemo (showofldemo.com) members spotlight their talents on a virtual stage, and the Instructables community (instructables.com) collaborates to provide instructions for arts, crafts, food, electronics, and games. Visit these Web sites and view the members’ products. Which items are popular? Which are unusual? Which photos provide details on documenting the steps necessary to complete a project? How do members share project ideas and requests for information? Summarize the information you read and viewed.</td>
</tr>
<tr>
<td><strong>Blogs</strong></td>
<td>More than 80,000 blogs are created daily according to Umbria Communications, a service that tracks new Internet media. Many information technology (IT) professionals maintain these blogs to tout companies’ products and express personal observations. IT bloggers include Robert Scoble on video (scobleizer.com); Jeff Jaffe, Novell’s chief technical officer (novell.com/cctoblog); Ed Brill on IBM (edbrill.com); and Tom Kyte on Oracle (tkyte.blogspot.com). Visit these blogs and read some of the posts. What new products are mentioned? What are the bloggers’ backgrounds? What controversial topics are discussed? What personal views do the bloggers express?</td>
</tr>
<tr>
<td><strong>Ethics in Action</strong></td>
<td>Radio frequency identification (RFID) tags are expected to help merchants in many ways. By placing these tags on such items as prescriptions, computer peripherals, and clothing, retailers hope to reduce theft, track inventory, reduce labor costs, and keep their shelves stocked. Privacy experts, however, claim the tags can store information about consumers’ shopping habits and whereabouts. Law enforcement officials, lawyers, marketers, and even thieves could use this detailed electronic data to track people at all times of the day. View Web sites that discuss using RFID tags in stores and the privacy issues that arise from their use. Write a report summarizing your findings, and include a table of links to Web sites that provide additional details.</td>
</tr>
</tbody>
</table>
Critical Thinking

The Critical Thinking exercises challenge your assessment and decision-making skills by presenting real-world situations associated with the chapter concepts. The Collaboration exercise should be completed with a team.

To discuss the Critical Thinking exercises with other students, visit scsite.com/dc2011/ch11/forum and post your thoughts or questions.

To evaluate the situations below, use personal experiences and available resources such as articles on the Web or in print, blogs, podcasts, videos, television, user guides, other individuals, and electronics and computer stores. You may need to use multiple resources to form conclusions and make recommendations.

1. Class Discussion — Unscrupulous Programmers
   Your best friend, Jonathon, spends all his free time writing computer programs that interact with the Windows operating system. He recently informed you that during fall break he had written malware that randomly erases files and displays weird messages the day before Independence Day (July 3) at exactly 1:00 p.m. He plans to distribute the Trojan horse, called Happy Birthday America, via an e-mail message. Also included with the e-mail message is a hidden program that sends the same e-mail message to all the e-mail addresses in the user’s address list. The e-mail message with the attachment will be sent as spam the day after finals in May, so that it will have ample time to be distributed to millions of computers worldwide before July 3. You know that a large software company offers a hefty reward of $250,000 for turning in unscrupulous programmers. Discuss if you think it is right to inform on a friend when no profit is involved in the crime. Include in your discussion who you would notify (i.e., Jonathon’s parents, the dean of students, the police, or the software company offering the reward) if you choose to turn him in.

2. Class Presentation — Ensuring Safety and Security Online
   You work in an information technology department for a large enterprise. You notice that an increasing number of users are contacting the help desk complaining of slow computer performance. When a help desk representative troubleshoots the problem, he or she nearly always attributes the decreased performance to malware that is installed on the computer. Although security software is installed on each computer, users also must do their part in making sure that their computers do not become compromised. Technical support is spending too much time and money troubleshooting and cleaning these computers. As a result, they have asked you to prepare a presentation for employees that will teach them how to guard against malware and other security threats. This presentation should include information such as which Web sites are safe and unsafe, whether it is okay to download programs from the Internet and install them, and how users can protect their computers when they are away from their desks.

3. Research — Threats to Operating Systems
   You work as a network analyst for a large manufacturing company that uses Windows. After the most recent virus attack, your manager asked you to analyze the feasibility of switching to a different operating system, such as Linux or UNIX. Use the Web and/or print media to research the advantages and disadvantages of switching operating systems. Create a report based on your findings to answer the following questions: Are alternative operating systems any less susceptible to viruses than Windows? Why or why not? What is Microsoft’s approach to eliminating virus attacks? What types of costs are involved in changing operating systems?

Collaboration

4. Privacy Information Policy
   Your company has been hired by a major retailer to create a privacy information policy for the company’s Web site. Your team of three classmates has been instructed to assemble a policy that not only respects an individual’s privacy rights but also enables the company to collect data that can be used in targeted marketing. The company would like to collect the following information: who visits the Web site, how often they visit, which pages they view, and the amount of time they spend viewing a particular page. Using the Web and/or print media, create a policy that will include all of the preceding information. Each team member should justify a component within the policy and explain how the policy will not violate the individual’s privacy rights. Include in your report examples of lawsuits brought against companies that have implemented similar policies. If any judgments were against the company, cite the specific reasons why.
FORENSICS USES SCIENCE to investigate and establish facts in criminal or civil courts. Digital forensics, the newest and fastest growing discipline in the forensics field, also can be referred to as computer forensics, network forensics, or cyberforensics. Digital forensics is the discovery, collection, analysis, and reporting of evidence found on computers and digital devices (Figure 1).

As a student in a digital forensics class, you will investigate a crime scene and observe law enforcement officials collecting evidence. After arriving at the crime scene, you expect a relatively short process that mainly involves confiscating a computer. You are surprised that the process of collecting evidence actually takes much longer than what is portrayed on the television shows you have watched.

This feature introduces students to digital forensics by presenting two real-world scenarios that involve the use of digital forensics. Throughout each scenario, students will learn the steps required to solve computer crimes by using digital forensics techniques.
Introduction to Digital Forensics

Digital forensics focuses on computers, digital devices, and networks, and requires the collection and analysis of digital evidence. Digital evidence exists on a variety of computers and digital devices, such as flash memory mobile media, external hard disks, cell phones, PDAs, copy machines, fax machines, answering machines, and GPS receivers. Depending on the type of crime, other digital devices, such as routers, portable media players, and digital cameras, also might need further examination for evidence that supports the criminal or civil case. Once the evidence is collected, law enforcement officials or digital forensics examiners will transport it to a forensics lab for investigation.

The forensic analysis of computers and digital devices specifically involves the examination of media, programs, and data and log files. Some computers and digital devices maintain log files, which track some or all activity on the computer or digital device. Digital forensics examiners use log files to reconstruct a perpetrator’s activity with a computer or digital device, such as instant messaging (IM) conversations, Internet chat room sessions, e-mail messages, Web sites visited, files opened, and image and video files viewed. The forensic analysis of networks focuses more on...
Homeland security uses digital forensics for civilian and military intelligence gathering.

Businesses and other private sector organizations use digital forensics to combat information security attacks.

Each of these areas uses the same core tools and skills in digital forensics.

Cybercrimes, which are online or Internet-based illegal acts, continue to increase in both the number of incidents and the amount of money stolen, largely because cybercriminals perceive these crimes to be less risky and more lucrative than street crimes such as burglary or theft. The average bank robber, for example, nets only a few thousand dollars, and most are caught and incarcerated. Conversely, cybercrimes such as credit card theft, identity theft, and financial scams tend to net larger sums of money, and the perpetrators are more difficult to catch and convict. The problem is compounded further by the fact that access to corporate network resources makes insider jobs by employees easier.

In addition to cybercrime, investigators also use digital forensics to combat terrorism. Terrorists around the world use computers and digital devices. Thus, digital forensics analysis is an important antiterrorism tool for both criminal prosecution and intelligence gathering.

As more people and organizations store information digitally and computers are increasingly integrated into more aspects of our society, we all face increased exposure and vulnerability.

**Digital Forensics Examiners**

As mentioned in Chapter 11, a digital forensics examiner must have knowledge of the law, technical experience with many types of hardware and software products, superior communication skills, familiarity with corporate structures and policies, a willingness to learn and update skills, and a knack for problem solving. Digital forensics covers several overlapping areas (Figure 2).

- Law enforcement uses digital forensics as an evidence gathering and criminal investigation tool.
- Homeland security uses digital forensics for civilian and military intelligence gathering.
- Businesses and other private sector organizations use digital forensics to combat information security attacks.

A digital forensics examiner must have knowledge of the law regardless of whether the investigation is for law enforcement or civilian purposes. Additional complexity in the law exists because computer crime statutes and users’ privacy expectations vary widely from state to state and nation to nation. Because the jurisdictional boundaries of the Internet are blurred, an individual in one country can commit crimes almost anywhere in the world without leaving his or her keyboard.

Although most digital forensics examiners today engage in law enforcement investigations, the field involves more than simply obtaining evidence against a criminal. Information security professionals employ digital forensics as well. The traditional information security manager proactively protects an organization’s information technology assets, such as computers and digital devices, peripherals, and storage media. Security intrusions and other events that jeopardize assets are inevitable, however. When an event compromises an asset, a digital forensics examiner often leads the incident response team to uncover how an event occurred, who was behind it, and how to prevent a recurrence. Third-party
Digital Forensics

Step 1 Gather the Materials to Analyze

The first step in the process is to gather the materials to analyze. A search warrant will guide law enforcement officials in the seizure of materials. Even with clear guidelines, law enforcement officials must consider many items for collection and examination. During this process, law enforcement personnel gather computer media, computers, mobile devices, peripherals, network hardware, and computer software.

Computer Media Media is available in a variety of forms (Figure 3). This includes hard disks, external hard disks, and optical discs. Also included are physically small, high-capacity memory devices such as USB flash drives (including versions of such devices disguised in a watch, pen, or Swiss Army knife, the last of which is shown in Figure 1 on page 607) and memory cards such as Secure Digital (SD) cards, CompactFlash cards, and xD Picture Cards.

Digital Forensics in Action

The complexity of the digital forensics process can vary, depending on the circumstances that initially caused the investigation. The digital forensics examiner may be part of an investigative team, with the analysis of digital evidence comprising just one part of the entire investigation. The examiner looks for information pertinent to the incident or event, which a search warrant, time, and/or other circumstances may limit. The following two scenarios illustrate how digital forensics is used to collect and analyze evidence for two cybercrimes.

Scenario 1: Identity Theft

Investigators suspect that Jonathan Nash is stealing identities and then opening credit card accounts to make fraudulent purchases online. At one point, Jonathan suspected that he was being investigated for this crime and attempted to delete all incriminating files on his computer. Before Jonathan can be charged with the crime, investigators will use digital forensics to prove that he is responsible for stealing the identities and making purchases using credit cards that belong to others.

Digital forensics examiners will perform several steps, discussed in the following pages, to collect evidence that can be used to convict Jonathan of this crime.

Scenario 2: Computer Crime

Every component of the computer needs to be considered for examination, and examiners generally confiscate any desktop and notebook computers; mobile devices such as smart phones, PDAs, and digital cameras; and peripherals such as keyboards and...
mouse devices (Figure 4). For example, examiners cannot assume that the keyboard in the forensics lab will be compatible with the computer being seized.

**GPS Receivers** Forensic examiners analyze an increasing number of GPS receivers each day. Examiners typically gather information such as the destinations that are programmed into the receiver, the locations where the receiver has been, and the route traveled. Some GPS receivers built into an automobile also record data about the vehicle’s performance, which also can help in an investigation.

**Network Hardware** Homes with broadband Internet connections increasingly have networks and, therefore, multiple computers, a router, and a wireless access point. Wireless networks allow criminals to hide a networked computer easily. For example, a notebook computer or mobile device using a home's wireless network can be as far as 100 yards from the wireless access point, and thus be far outside of the immediate structure. Furthermore, the suspect may be stealing a neighbor's wireless network while engaging in criminal activity.

**Computer Software** Digital forensics examiners generally will not run software directly from the suspect hard disk because it might add, change, or remove data on the hard disk that is important for the investigation. Instead, they copy the data to another storage medium and use software at the forensics lab to access the data. In cases where the examiner does not have access to specialized, custom, or old software on the suspect’s computer, the examiner may have to install software found at the suspect’s site on a computer in the forensics lab. For this reason, examiners should seize program discs and manuals for any software with which they are unfamiliar. Any papers and books near the suspect's computer also will give the examiner a clue as to the sophistication of the user and the possible types of programs on the computer.

**Scenario Specifics**

In the case of Jonathan Nash, law enforcement officials obtained a search warrant to enter Jonathan’s house and confiscate specific items. Officials locate an office with a computer and peripheral device that writes data on magnetic stripes. Law enforcement officials also locate various storage media, which might contain personal information or credit card information.

**Step 2 Transport the Materials**

Once the materials are gathered, law enforcement officials or digital forensics examiners transport them safely to a forensics lab where digital forensics examiners will examine the media for information related to the crime.

**Scenario Specifics**

Law enforcement officials carefully package the computer and digital devices they have obtained from Jonathan’s office so that no damage will occur during transport.

![Figure 4 Common digital hardware devices examined by a digital forensics examiner.](image-url)
Step 3 Preserve the Media

The next step in the investigation is preserving the media. Where possible, examiners should not perform digital forensics analysis on the original media, because of the potential of accidentally changing the original evidence. Thus, the examiners typically make a copy of all media, ensuring that they do not alter the original data and information in any way and that the copy will be authenticated as identical to the original. This process is known as creating an image, or imaging.

In the extraordinary circumstances when the examiner must analyze the original media, such as a hard disk, they often use a write-protection device. A write-protection device prevents the examiner or the computer from inadvertently writing data and information on the media (Figure 5). Write-protection devices can cost from several hundred to several thousand dollars, depending on the types of media to which it can connect.

In some cases, examiners may create an image of a hard disk at the crime scene rather than transporting entire computers to the forensics lab. This is the preferable approach when the disk to be imaged is on a company’s critical server and/or where seizing the computer might cause undue economic hardship to the owner. Devices such as Intelligent Computer Solutions’ Road MASSter-3 fit in a small carrying case and are designed to image hard disks in the field (Figure 6).

Notebook computer hard disks represent a particular challenge for forensic analysis because many have proprietary or specialty interfaces. Additional hardware is available specifically for imaging drives for various models of Dell, Acer, HP, Lenovo, NEC, Toshiba, and other brands of notebook computers. Other specialized hardware allows for the imaging of smart phones, PDAs, and other mobile devices.

Scenario Specifics

The digital forensics examiner does not want to damage or change the original data on Jonathan’s hard disk, so he creates an image of the hard disk. During the imaging process, a write-protection device ensures that nothing inadvertently is written to the original hard disk.

Step 4 Extract Evidence

The next step in the investigation requires the digital forensics examiner to extract the evidence from the media. Based on the guidelines of the investigation, the examiner determines the type of data and information on the computer that is pertinent to the case. In a case of suspected child exploitation, photos and videos are important. Chat room and e-mail logs are useful in cyberstalking cases because they might contain incriminating conversations involving the suspect. Some cybercriminals attempt to delete some or all files on their hard disk in an attempt to hide their illicit or illegal behavior. Examiners analyzing the media, however, usually are able to recover deleted files by

---

Figure 5  Write-protection devices prevent examiners from inadvertently altering digital evidence.

Figure 6  Shown here are details of the keyboard and working area of Intelligent Computer Solutions’ Road MASSter-3, a portable digital forensics laboratory.
The next step, analyzing the evidence and/or determining the root cause of the event, is the most time-consuming aspect of the process. The data and information that an examiner retrieves from the computer either can be incriminating (indicating guilt) or exculpatory (indicating innocence). Additionally, the examiner looks at the entire capacity of the medium because data and information can be hidden anywhere, including locations on the medium that appear empty. Figure 8 summarizes the common items examined during a digital forensics investigation.

**Step 5 Analyze Evidence**

In this case, Jonathan attempted to delete the incriminating files but was not aware of tools that would permanently erase them. The digital forensics examiner is able to locate remnants of the files on the hard disk and is able to restore them nearly to their original form. Although the files have not been restored fully, the digital forensics examiner is able to restore enough data to retrieve potentially incriminating evidence.

**Scenario Specifics**

In this case, Jonathan attempted to delete the incriminating files but was not aware of tools that would permanently erase them. The digital forensics examiner is able to locate remnants of the files on the hard disk and is able to restore them nearly to their original form. Although the files have not been restored fully, the digital forensics examiner is able to restore enough data to retrieve potentially incriminating evidence.

**Figure 7** The top portion of this figure shows the suspect (a) listing the files involved in criminal activity and (b) later deleting the files in an attempt to cover up the illegal activity. The lower portion of the figure shows (c) the digital forensics examiner retrieving the deleted files using special programs.

**Figure 8** The common items examined during a digital forensics investigation.
Digital Forensics Tools  As previously mentioned, examiners use digital forensics tools to perform an analysis to ensure that no information is modified on the target media and that the examination is thorough. When a computer starts, hundreds of registry, log, and/or data files may change. Examiners never should use a suspect’s disk to start a computer. Additionally, many operating systems, such as Windows, UNIX, and Linux, maintain a number of time stamps associated with every file, including the creation, last access, and last modified dates. Using ordinary utility programs to examine the contents of files usually will alter at least the last access date. Specialized analysis tools maintain the integrity of the original data so that the examiner can be sure that the results of the analysis are legally and technically valid and that nothing harms the original evidence.

A wide variety of digital forensics tools is available, each with its own use, strengths, and weaknesses. Several companies make digital forensics hardware, primarily for purposes of creating disk images. Digital Intelligence, for example, provides several forensic hardware devices, including the following:

- Forensic Recovery of Digital Evidence (FRED) is a stand-alone forensics workstation that can acquire data from all types of hard disk media, including EIDE, ATA, SATA, SAS, and SCSI hard disks (Figure 9a). This unit includes fixed hard disks for the workstation’s operating system and analysis tools along with a number of bays so that forensic examiners can insert and remove other drives. For imaging situations, the examiner copies the contents of the suspect disk to a blank disk; the examiner then performs analysis on the newly copied disk.
- The Forensic Duplicator replication hardware allows the examiner to connect IDE and SATA hard disks and can replicate the contents of one disk to another (Figure 9b). The examiner also can copy the contents of one disk to a file.
- FireFly is a device that plugs directly into an EIDE, IDE, SAS, or SATA hard disk and attaches to the forensic computer via a FireWire connection (Figure 9c).

The primary digital forensics analysis tool is software. The most widely-used specialty forensic programs today are Guidance Software’s EnCase and AccessData’s Forensic Toolkit, also known as FTK, which assist in gathering and
Analyzing Mobile Devices  Forensic examination increasingly requires analysis of mobile devices such as smart phones, PDAs, digital cameras, and portable media players. The amount of personal information on smart phones and PDAs, for example, includes contact lists, call history, text messages, photos and videos, e-mail messages, calendars, and documents. In some ways, analysis of mobile devices is more problematic than analysis of desktop and notebook computers, because mobile devices use a wide variety of connectors, operating environments, file structures, data formats, features, user interfaces, and operating modes. Mobile devices also can contain a variety of expansion cards including flash memory mobile media and Subscriber Identity Module (SIM) cards.

Examiners also can use mobile devices to pinpoint a person's or device's whereabouts and routes traveled. GPS is becoming more prevalent in mobile devices. Systems like OnStar use GPS technology to determine a vehicle's precise location.

Analyzing Chat Room Logs  Analysis of chat room logs is another important aspect of network analysis. The log shown in Figure 1 on page 607 is a conversation between BettyF, billy89, and other members of the Internet Relay Chat (IRC) Strong&40 channel. Analysis of logs such as these can uncover evidence of cyberstalking, criminal conspiracy, harassment, or other topics of interest to the examiner.

Analyzing Browser History Logs  Occasionally, it is necessary to trace a user's Web browsing path. Manual forensic analysis, which involves searching through cookies, the browser's cache, and browser history data, is difficult. Several programs are available to analyze a browser's history, although most new browsers include an incognito mode that prevents the browser from storing Web pages and addresses in the history. Some programs can locate and reconstruct file fragments from the Recycle Bin folder on the Windows desktop.

**Scenario Specifics**
The digital forensics examiner is attempting to locate evidence on Jonathan's hard disk that will help convict him of identity theft. In this case, the examiner has found documents and spreadsheets containing credit card numbers, saved Web pages showing receipts for items purchased, and browser history logs indicating that Jonathan regularly visited Web sites that sell stolen credit card numbers.

**Step 6  Document Results**
The final step in the investigation is to document the results of a digital forensics examination thoroughly, particularly when performing the examination for legal purposes. It is important to document everything, including the computer configuration and BIOS settings, the steps taken by the digital forensics examiner, and any pertinent evidence. All computer equipment, media, peripherals, or other items seized must be logged, and examiners should take photos of external and internal connections, when possible. The examiner carefully logs the handling of the evidence to demonstrate that no tampering occurred. Sample digital forensics evidence worksheets are shown in Figure 12. Figure 12a shows an evidence worksheet used when analyzing a computer. Figure 12b contains evidence worksheets used when analyzing a hard disk.

**Scenario Specifics**
The evidence on Jonathan Nash's hard disk and other media determine whether he is guilty of identity theft; however, the precision in collecting and analyzing the evidence is critical if it is to be admissible in a court case.
Scenario 2: Spam Attacks

Someone is sending an unusually large number of unsolicited e-mail messages to employees of a well-known insurance company. The company’s spam filter is not able to remove each message, and employees are spending too much time removing unwanted e-mail messages. As a result, employees sometimes inadvertently remove legitimate e-mail messages. The increased e-mail messages are decreasing network performance and causing the company to lose money. It is important to locate and stop those responsible for sending the unsolicited e-mail messages.

The origin of the attacks initially is unknown, because the e-mail messages appear to come from many different e-mail addresses, although the content of each message is similar. Digital forensics examiners must rely on information provided by the attacked company. The previous scenario listed six steps describing how to locate, analyze, and document the evidence. This scenario is somewhat more complex because it is not known who is responsible for the attacks.

In this scenario, a digital forensics examiner might use the following techniques to locate the attacker and/or the computer network facilitating the attacks. Once the examiner finds the attacker, he or she might use the six steps in the previous scenario to link the attacker to the crime.

Analyzing Network Traffic The ability to analyze network traffic is an essential skill for a digital forensics examiner. E-mail headers are particularly important, as they provide many clues as to the origin and authenticity of e-mail messages. E-mail headers, which do not display in the body of the e-mail message, usually include the standard To:, From:, and Subject: lines. E-mail headers contain more information, however, than what appears at the top of an e-mail message. For example, they also can reveal the name and version of the e-mail program that created an e-mail message, the operating system used to create the e-mail message, the name and version of the mail server, internal IP addresses, and the mail server path taken by a message.
Tracking Packet Routes  Examiners also must have knowledge of how the Internet works. Figure 13a shows the results from VisualRoute, listing the intermediate packet routes between a local host computer and a Web server (www.fujifilm.co.jp). VisualRoute is a utility program that lists the IP address and location of all routers with which it communicates along the path between the two computers. VisualRoute also can show a geographic map of the path (Figure 13b).

Analyzing Internet Access Provider Logs  During a digital forensics investigation, the examiner might request logs from an Internet access provider. The Internet access provider will deliver the logs, but they will be in the raw format in which they are saved.

While the SMTP protocol forwards e-mail messages across the Internet, other protocols download e-mail messages by e-mail programs. One such protocol is the Post Office Protocol version 3 (POP3). Figure 1 on page 607 shows a set of three records from a POP3 server log showing a user logging on to check and download e-mail messages. All records show a date (February 12) and time stamp on a host named watson running the POP3 service (pop3d) and access by a user on the host with IP address 192.168.187.35.

Analyzing a Packet Trace  Packet sniffers are an important software tool in understanding network traffic. A packet sniffer monitors all of the traffic seen on the network port of a computer and retains a copy for later analysis. One of the most commonly used packet sniffers is tcpdump, a program for the UNIX and Linux operating systems. WinDump is the Windows version of the program.

Scenario Specifics

Digital forensics examiners were able to analyze the company’s logs, as well as e-mail headers from the unwanted e-mail messages. The e-mail headers led officials to an Internet access provider in Europe. Upon requesting logs from the European Internet access provider, officials find that the IP address used to send the e-mail messages was assigned to an individual who ultimately was not aware of the crime. His computer, however, was being used as a zombie; that is, a computer controlled by an outsider without the owner’s knowledge. The individual was able to help resolve the problem by locating and removing the malicious software from his computer.

Learning More about Digital Forensics

Every action a user takes on a computer or digital device leaves a trail. Deleting files really does not erase information; instead, it tells the computer that it can write new data to the space. Evidence of computer activity is stored in many places on the hard disk, some obvious and some obscure. Information about network access potentially is logged on many computers throughout the local network and global Internet. Evidence of your activities on computers and digital devices is everywhere. Using popular search engines such as Google, Yahoo!, Bing, and others, you will find links to hundreds of digital forensics sites. For a list of sources for information about digital forensics, visit scsite.com/dc2011/ch11/digitalforensics.