DIGITAL SECURITY, ETHICS, AND PRIVACY: Threats, Issues, and Defenses

5

Users should take precautions to protect their digital content.

"I am careful when browsing the web, use antivirus software, and never open email messages from unknown senders. I use a cloud storage provider to back up my computer and mobile devices. What more do I need to know about digital safety and security?"

While you may be familiar with some of the content in this chapter, do you know how to . . .

- Avoid risks when playing online games?
- Determine if an email message has been spoofed?
- Tell if your computer or device is functioning as a zombie?
- Set up a personal firewall?
- Protect computers and devices from viruses and other malware?
- Protect your passwords?
- Use two-step verification?
- Prevent your data from being lost on the cloud?
- Follow a disaster recovery plan?
- Secure your wireless network?
- Safeguard your hardware and data from a disaster?
- Protect against a phishing scam?
- Protect yourself from social engineering scams?
- Evaluate your electronic profile?

In this chapter, you will discover how to perform these tasks along with much more information essential to this course. For additional content available that accompanies this chapter, visit the free resources and premium content. Refer to the Preface and the Intro chapter for information about how to access these and other additional instructor-assigned support materials.

Objectives

After completing this chapter, you will be able to:

1. Define the term, digital security risks, and briefly describe the types of cybercriminals
2. Describe various types of Internet and network attacks (malware, botnets, denial of service attacks, back doors, and spoofing) and explain ways to safeguard against these attacks, including firewalls
3. Discuss techniques to prevent unauthorized computer access and use, including access controls, user names, passwords, possessed objects, and biometric devices
4. Explain ways that software manufacturers protect against software piracy
5. Discuss how encryption, digital signatures, and digital certificates work
6. Identify safeguards against hardware theft, vandalism, and failure
7. Explain options available for backing up
8. Identify risks and safeguards associated with wireless communications
9. Recognize issues related to information accuracy, intellectual property rights, codes of conduct, and green computing
10. Discuss issues surrounding information privacy, including electronic profiles, cookies, phishing, spyware and adware, social engineering, privacy laws, employee monitoring, and content filtering

Digital Security Risks

Today, people rely on technology to create, store, and manage their critical information. Thus, it is important that computers and mobile devices, along with the data and programs they store, are accessible and available when needed. It also is crucial that users take measures to protect or safeguard their computers, mobile devices, data, and programs 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 numbers are secure when they make online purchases.

A **digital security risk** is any event or action that could cause a loss of or damage to computer or mobile device hardware, software, data, information, or processing capability. The more common digital security risks include Internet and network attacks, unauthorized access and use, hardware theft, software theft, information theft, and system failure (Figure 5-1).

While some breaches to digital security are accidental, many are intentional. Some intruders do not disrupt a computer or device's functionality; they merely access data, information, or programs on the computer or mobile device before signing out. Other intruders indicate some evidence of their presence either by leaving a message or by deliberately altering or damaging data.

Cybercrime

An intentional breach to digital security often involves a deliberate act that is against the law. Any illegal act involving the use of a computer or related devices generally is referred to as a **computer crime**. The term **cybercrime** refers to online or Internet-based illegal acts such as distributing malicious software or committing identity theft. Software used by cybercriminals sometimes is called *crimeware*. Today, combating cybercrime is one of the FBI's top priorities.

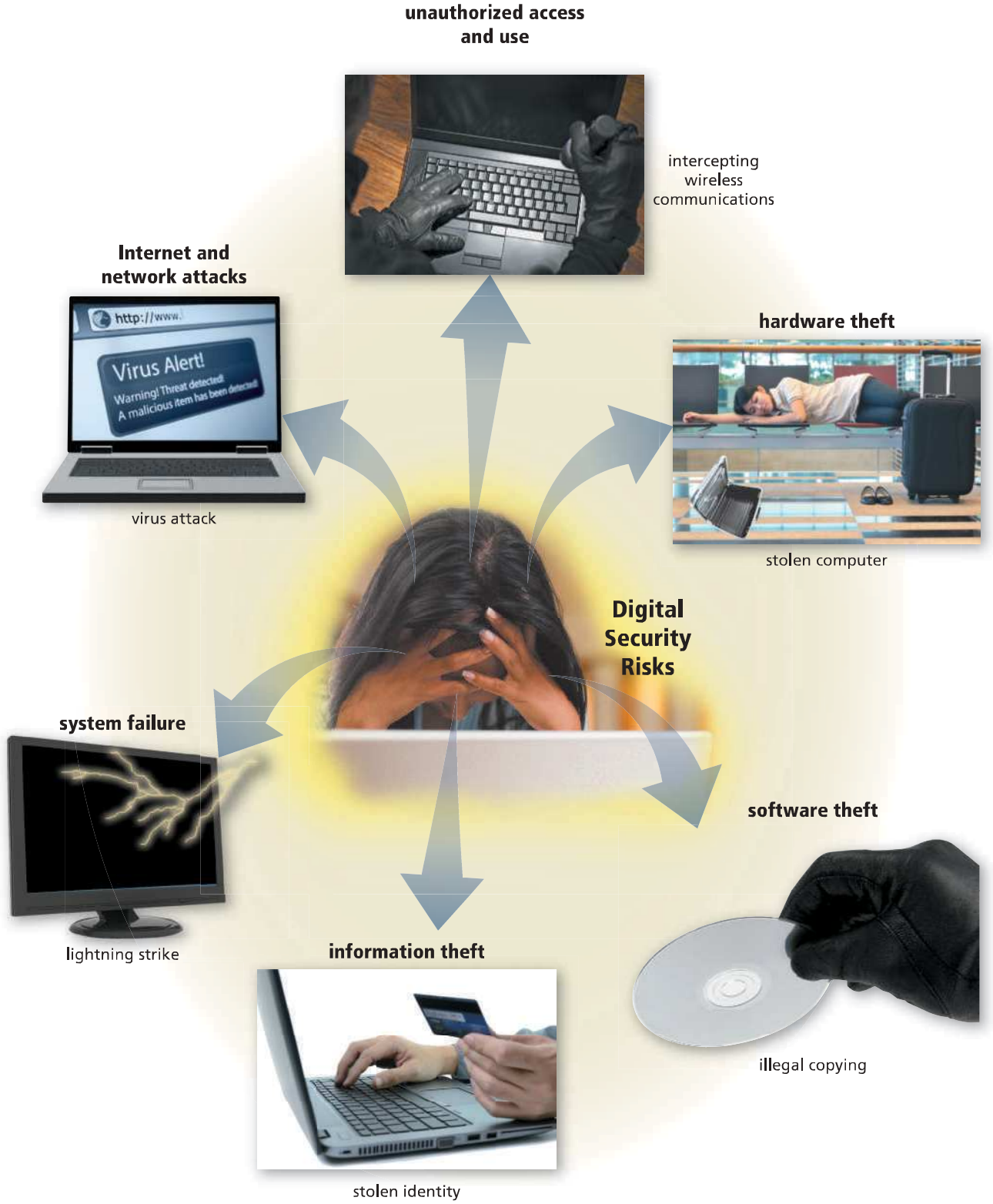


Figure 5-1 Computers and mobile devices, along with the data and programs they store, are exposed to several types of digital security risks.

Perpetrators of cybercrime typically fall into one of these 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 and networks.
- 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 demands payment to stop an attack on an organization's technology infrastructure. These perpetrators threaten to 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.

Internet Research
How do script kiddies use malware?
Search for: script kiddie malware

Read Ethics & Issues 5-1 to consider how cybercriminals should be punished. 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.

Discover More: Visit this chapter's free resources to learn more about cybercriminals.

ETHICS & ISSUES 5-1

How Should Cybercriminals Be Punished?

A hacker received a 10-year jail sentence for selling credit card information from several large corporations, costing one company approximately $200 million. In another case, a hacker accessed the personal online accounts of celebrities, as well as people he knew, and distributed revealing photos and information. He also received 10 years in jail, in part for the emotional distress his actions caused his victims. Do these sentences seem too harsh? Some legal experts point out that the punishment given to some hackers is not in line with crimes of a violent nature.

In addition to the extent of the punishment, other issues surrounding cybercrime laws include whether an action is defamation or free speech and who should be punished, the hacker or those who were hacked. If a hacker's actions damage the reputation of another via libel or slander, should the hacker be prosecuted under the defamation law or be protected under the First Amendment? A *hacktivist*, which is a type of hacker whose actions are politically or socially motivated, believes his or her actions should be protected under the First Amendment. Should companies whose systems have been breached be punished for their lax security? The Federal Trade Commission (FTC) has fined companies whose security flaws enabled hackers to access their systems.

Legislators have made efforts to define and prevent cybercrime, both with new laws and the expansion of existing laws. Cybercrime laws vary between states and countries, making it difficult to establish what is illegal. Determining who has jurisdiction over a case can create more legal hassles. For example, which area is responsible for determining punishment: where the victim(s) resides or where the criminal lives?

Consider This: Should hacktivism be punishable? Why or why not? Should corporations be liable for damages caused by hackers? Why or why not? Should hackers receive comparable punishment to violent criminals? Why or why not?

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. Internet and network attacks that jeopardize security include malware, botnets, denial of service attacks, back doors, and spoofing.

Internet Research
Does a list of known malware exist?
Search for: malware list

Malware

Recall that **malware**, short for *malicious software*, consists of programs that act without a user's knowledge and deliberately alter the operations of computers and mobile devices. Table 5-1 summarizes common types of malware, all of which have been discussed in previous chapters. Some malware contains characteristics in two or more classes. For example, a single threat could contain elements of a virus, worm, and trojan horse.

Malware can deliver its *payload*, or destructive event or prank, on a computer or mobile device in a variety of ways, such as when a user opens an infected file, runs an infected program, connects an unprotected computer or mobile device to a network, or when a certain condition or event occurs, such as the computer's clock changing to a specific date. A common way that computers and mobile devices become infected with viruses and other malware is through users opening infected email attachments (Figure 5-2). Read Secure IT 5-1 to learn about how malware can affect online gaming.

Table 5-1 Common Types of Malware

Type	Description
Virus	A potentially damaging program that affects, or infects, a computer or mobile device negatively by altering the way the computer or device works without the user's knowledge or permission.
Worm	A program that copies itself repeatedly, for example in memory or on a network, using up resources and possibly shutting down the computer, device, or network.
Trojan horse	A program that hides within or looks like a legitimate program. Unlike a virus or worm, a trojan horse does not replicate itself to other computers or devices.
Rootkit	A program that hides in a computer or mobile device and allows someone from a remote location to take full control of the computer or device.
Spyware	A program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online.
Adware	A program that displays an online advertisement in a banner, pop-up window, or pop-under window on webpages, email messages, or other Internet services.

Discover More: Visit this chapter's free resources to learn more about malware.

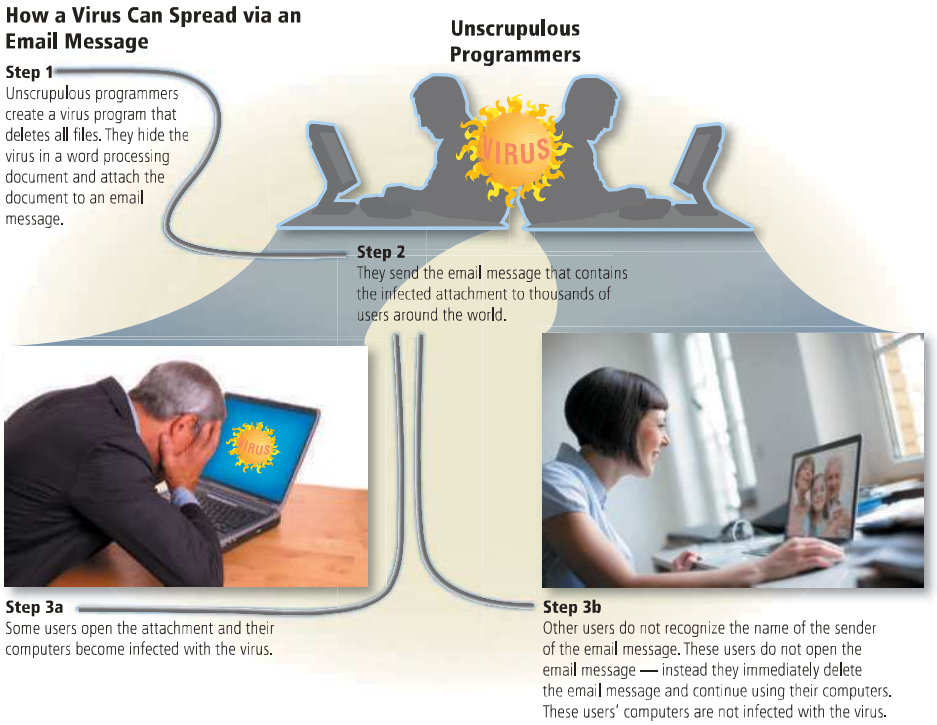


Figure 5-2 This figure shows how a virus can spread via an email message.

Internet Research
What are the latest malware threats?
Search for: malware news

CONSIDER THIS

What if you cannot remove malware?
In extreme cases, in order to remove malware from a computer or mobile device, you may need to erase, or reformat, an infected computer's hard drive, or reset a mobile device to its factory settings. For this reason, it is critical you have uninfected (clean) backups of all files. Consider creating recovery media when you purchase a new computer, and be sure to keep all installation media in the event you need to reinstall the computer's operating system and your apps. Seek advice from a technology specialist before performing a format or reformat instruction on your media.

SECURE IT 5-1

Play It Safe to Avoid Online Gaming Risks

Gamers often understand general security issues regarding online behavior, but they may not be aware of a different set of technology and social risks they may encounter as they interact in the online world. Anyone experiencing the joys of playing games online or playing games with others through online services should realize that thieves and hackers lurking behind the scenes may take advantage of security holes and vulnerabilities that can turn a gaming session into a nightmare.

Viruses, worms, and malware can be hidden in downloaded game files, mobile apps, email message attachments, and messaging software. In addition, messages on online social networks may encourage gamers to visit fraudulent websites filled with malware. If the game requires a connection to the Internet, then any computer connected to the game's server is subject to security cyberthreats. Thieves can take control of a remote computer that does not have a high level of security protection and use it to control other computers, or they could break into the computer and install malware to discover personal information.

Malicious users know that the gaming community uses social media intensely, so they also create accounts and attempt to mislead uninformed users into revealing personal information. The thieves may claim to have software updates and free games, when they really are luring users to bogus websites that ask users to set up profiles and accounts.

Gamers should follow these practices to increase their security:

- Before downloading any software or apps, including patches to games, or disclosing any private details, check the developer to be certain the website or the person making the request is legitimate.
- Read the permissions notices to learn what information is being requested or being collected. Avoid games requiring passwords to be saved to an online account on a smartphone.
- Exercise extreme caution if the game requires ActiveX or JavaScript to be enabled or if it must be played in administrator mode.
- Use a firewall and make exceptions to allow only trusted individuals to access your computer or mobile device when playing multiplayer online games.
- Do not share personal information with other gamers whom you meet online.

Consider This: Have you played online games or downloaded gaming apps and followed the advice listed here? How will you change your gaming behavior now that you are aware of specific security threats?

Botnets

A **botnet**, or *zombie army*, is a group of compromised computers or mobile devices connected to a network, such as the Internet, that are used to attack other networks, usually for nefarious purposes. A compromised computer or device, known as a **zombie**, is one whose owner is unaware the computer or device 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 and devices to create a botnet. The perpetrator then uses the botnet to send spam via email, spread viruses and other malware, or commit a distributed denial of service attack (discussed in the next section).

CONSIDER THIS

How can you tell if your computer or mobile device is functioning as a zombie?
Your computer or mobile device may be a zombie if you notice an unusually high drive activity, a slower than normal Internet connection, or connected devices becoming increasingly unresponsive. The chances of your computer or devices becoming part of a botnet greatly increase if your devices are not protected by an effective firewall.

Denial of Service Attacks

A **denial of service attack** (**DoS attack**) is an assault whose purpose is to disrupt computer access to an Internet service, such as the web or email. 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 *distributed DoS attack* (*DDoS 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 websites, including powerhouses such as Yahoo!, eBay, Amazon.com, and CNN.com.

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

Internet Research
Are DoS attacks still prevalent?
Search for: news of dos attacks

CONSIDER THIS

Why would someone execute a Dos or DDoS attack?
Perpetrators have a variety of motives for executing a DoS or DDoS attack. Hactivists, or 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.

Back Doors

A **back door** is a program or set of instructions in a program that allows 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 spam 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. Two common types of spoofing schemes are IP and email spoofing.

- *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 website. For example, the victim may provide confidential information or download files containing viruses, worms, or other malware.
- *Email spoofing* occurs when the sender's address or other components of an email header are altered so that it appears that the email message originated from a different sender. Email spoofing commonly is used in virus hoaxes, spam, and phishing scams (Figure 5-3). Read How To 5-1 to learn about how to determine if an email message has been spoofed.

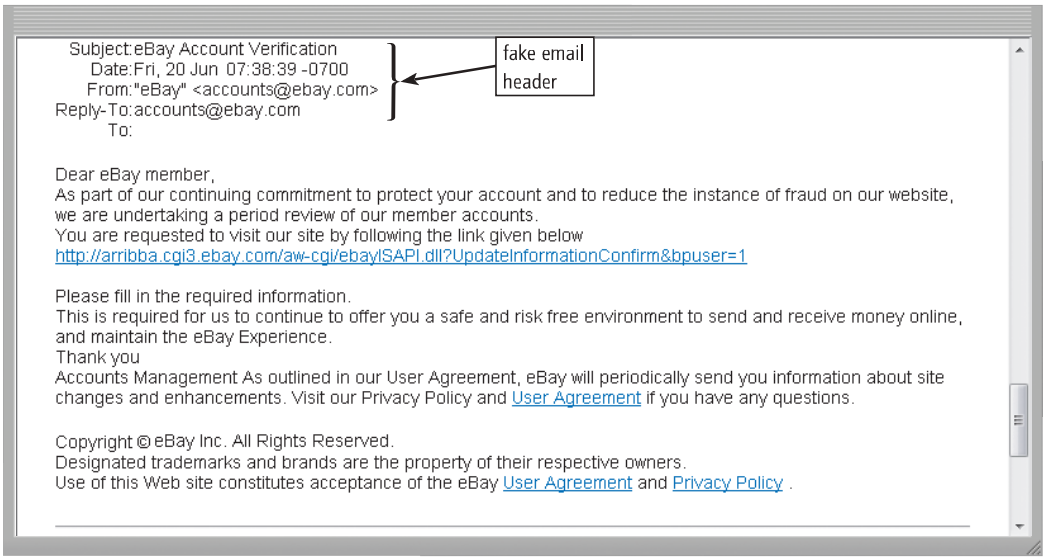


Figure 5-3 With email spoofing, the components of an email header are altered so that it appears the email message originated from a different sender.
Source: Privacy Rights Clearinghouse

HOW TO 5-1

Determine If an Email Message Has Been Spoofed

Spoofed email messages appear to originate from one source, but in reality originate from another source. Spoofed email messages often are sent by nefarious people attempting to obtain personal information. For example, an email message appearing to be sent from a reputable source, such as your financial institution, may ask you to reply with personal information, such as a password, Social Security number, or account number. If you reply, you will be sending personal information to an unknown third party that could use the information to steal your identity, make unauthorized purchases, and more. The following steps describe some ways to determine if an email message has been spoofed.

- The email message requests personal information, such as account numbers, passwords, Social Security numbers, and credit card numbers.
- The email message contains spelling and/or grammatical errors.
- The email message encourages you to tap or click a link that takes you to another website.
- The header in the email message contains a different domain in the MessageID than the domain of the supposed sender.
- The "From" and "Reply-To" email addresses do not match.

If you ever are unsure of whether an email message was spoofed, contact the supposed sender either via phone or a new email message (do not reply to the original email message) to verify the authenticity of the message.

Consider This: Have you ever received a spoofed email message? Did you know it was spoofed? What steps did you take?

Safeguards against Internet and Network Attacks

Methods that protect computers, mobile devices, and networks from attacks include the following:

- Use antivirus software.
- Be suspicious of unsolicited email attachments.
- Scan removable media for malware before using it.
- Implement firewall solutions.
- Back up regularly.

Secure IT 1-2 in Chapter 1 provided some measures you can take to protect your computers and mobile devices from malware. Read Secure IT 5-2 for additional tips to protect home users against Internet and network attacks. The next section discusses firewalls in more depth.

BTW

Antivirus Programs

In addition to protecting against viruses and other malware, many antivirus programs also include protection from DoS and DDoS attacks.

SECURE IT 5-2

Protection from Viruses and Other Malware

It is impossible to ensure a virus or malware never will attack a computer, but you can take steps to protect your computer by following these practices:

- **Use virus protection software.** Install a reputable antivirus program and then scan the entire computer to be certain it is free of viruses and other malware. Update the antivirus program and the virus signatures (known specific patterns of viruses) regularly.
- **Use a firewall.** Set up a hardware firewall or install a software firewall that protects your network's resources from outside intrusions.
- **Be suspicious of all unsolicited email and text messages.** Never open an email message unless you are expecting it, *and* it is from a trusted source. When in doubt, ask the sender to confirm the message is legitimate before you open it. Be especially cautious when deciding whether to tap or click links in email and text messages or to open attachments.
- **Disconnect your computer from the Internet.** If you do not need Internet access, disconnect the computer from the Internet. Some security experts recommend disconnecting from the computer network before opening email attachments.
- **Download software with caution.** Download programs or apps only from websites you trust, especially those with music and video sharing software.
- **Close spyware windows.** If you suspect a pop-up or pop-under window may be spyware, close the window. Never tap or click an Agree or OK button in a suspicious window.
- **Before using any removable media, scan it for malware.** Follow this procedure even for shrink-wrapped software from major developers. Some commercial software has been infected and distributed to unsuspecting users. Never start a computer with removable media inserted in the computer unless you are certain the media are uninfected.
- **Keep current.** Install the latest updates for your computer software. Stay informed about new virus alerts and virus hoaxes.
- **Back up regularly.** In the event your computer becomes unusable due to a virus attack or other malware, you will be able to restore operations if you have a clean (uninfected) backup.

Consider This: What precautions do you take to prevent viruses and other malware from infecting your computer? What new steps will you take to attempt to protect your computer?

CONSIDER THIS

How can you determine if your computer or mobile device is vulnerable to an Internet or network attack? You could use an **online security service,** which is a web app that evaluates your computer or mobile device to check for Internet and email vulnerabilities. The online security service then provides recommendations of how to address the vulnerabilities.

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

Discover More: Visit this chapter's free resources to learn more about online security services.

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. All networked and online 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 in and out of 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 (discussed later in this chapter).

BTW
Technology Innovators
Discover More: Visit this chapter's free resources to learn about AVG, Intel Security, and Symantec (security product developers).

Home and small/home office users often protect their computers with a personal firewall. As discussed in Chapter 4, a **personal firewall** is a software firewall 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 intrusions. Both Windows and Mac operating systems include firewall capabilities, including monitoring Internet traffic to and from installed applications. Read How To 5-2 for instructions about setting up a personal firewall.

Some small/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 a personal firewall. Hardware firewalls stop malicious intrusions before they attempt to affect your computer or network. Figure 5-4 illustrates the purpose of hardware and software firewalls.

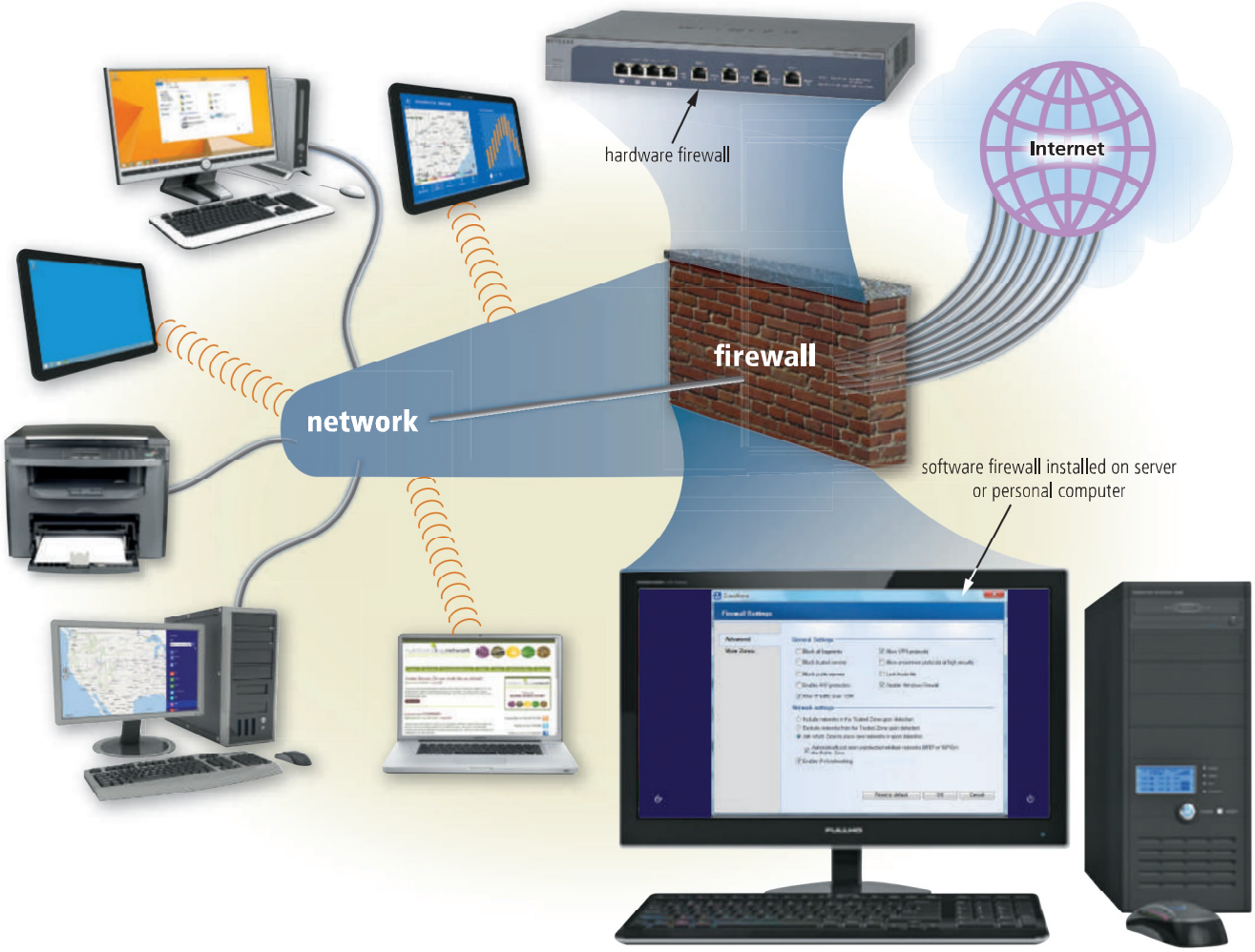


Figure 5-4 A firewall is hardware and/or software that protects a home or business's network resources from intrusion by users on another network, such as the Internet.

Courtesy of NETGEAR; © Cengage Learning; Courtesy of CheckPoint Software Technologies; © iStockphoto / Skip Odonnell; Source: Nutrition Blog Network; © iStockphoto / 123render; Source: Microsoft; © Iakov Filimonov / Shutterstock.com; © iStockphoto / Oleksiy Mark; Source: Microsoft; © iStockphoto / Ayaaz Rattansi; Source: Microsoft; © iStockphoto / Oleksiy Mark; Source: Microsoft; © Cengage Learning; Microsoft

HOW TO 5-2

Set Up a Personal Firewall

A personal firewall is a program that helps protect your computer from unauthorized access by blocking certain types of communications. For example, if somebody knows the IP address of your computer and attempts to access it using a browser or other program, the personal firewall can be configured to deny the incoming connection. The following steps describe how to set up a personal firewall.

1. Locate and purchase a personal firewall. You can purchase personal firewalls online and in stores that sell software. Many operating systems include a personal firewall. Computers typically can have only one active personal firewall running at a time. If you purchase a personal firewall, you may need to disable the one that is included with the operating system.
2. If you purchase a personal firewall, follow the instructions to install the program on your computer.
3. Run the personal firewall.
4. If necessary, ensure the personal firewall is enabled.
5. Review the settings for the incoming and outgoing rules. Incoming rules display programs and services that are allowed to access your computer. Outgoing rules display programs and services on your computer that are allowed to communicate with other computers and mobile devices on your network or the Internet.
6. Back up or export your current list of incoming and outgoing rules. If your computer does not function properly after you adjust the rules (in Steps 7 and 8), you will be able to restore the current rules.
7. Adjust your incoming rules to disallow devices, programs, and services you do not want accessing your computer. Be careful adjusting these settings, as adding or removing rules may hinder a legitimate program's capability to work properly.
8. Adjust your outgoing rules to allow only appropriate programs on your computer to communicate with other computers and mobile devices on your network or the Internet. Examples include a browser, email program, or other communications programs.
9. Save your settings.
10. Test programs on your computer that require Internet access. If any do not function properly, restore the list of rules you backed up or exported in Step 6.
11. Exit the personal firewall.

Consider This: Which programs on your computer should have access to the Internet? Which programs should not?

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.

Home and business users can be a target of unauthorized access and use. Unauthorized use includes a variety of activities: an employee using an organization's computer to send personal email messages, an employee using the organization's word processing software to track his or her child's soccer league scores, or a perpetrator gaining access to a bank computer and performing an unauthorized transfer.

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 activities for which the computer and network may and may not be used. An organization's AUP should specify the acceptable use of technology 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. The AUP also should specify the personal activities, if any, that are allowed on company time. For example, can employees check personal email messages or respond to personal text messages during work hours?

To protect your personal computer from unauthorized intrusions, you should disable file and printer sharing in your operating system (Figure 5-5). This security measure attempts to ensure that others cannot access your files or your printer. You also should be sure to use a firewall. The following sections address other techniques for protecting against unauthorized access and use. The technique(s) used should correspond to the degree of risk that is associated with the unauthorized access.

Figure 5-5 To protect files on your device's hard drive from hackers and other intruders, turn off file and printer sharing on your device.
Source: Microsoft

Access Controls

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, mobile device, or network. An *access control* is a security measure that defines who can access a computer, device, or network; when they can access it; and what actions they can take while accessing it. In addition, the computer, device, or network 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 perpetrator 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. The security program can be configured to alert a security administrator whenever suspicious or irregular activities are suspected. In addition, an organization regularly should review users' access privilege levels to determine whether they still are appropriate.

User Names and Passwords

A **user name** — also called a *user ID* (identification), log on name, or sign in name — 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.

Figure 5-6 Many websites that maintain personal and confidential data, such as Citibank's credit card system, require a user to enter a user name (user ID) and password.
Source: Citigroup Inc

Most operating systems that enable multiple users to share computers and devices or that access a home or business network require users to enter a user name and a password correctly before they can access the data, information, and programs stored on a computer, mobile device, or network. Many systems that maintain financial, personal, and other confidential information also require a user name and password as part of their sign-in procedure (Figure 5-6).

Some systems assign a user name and/or password to each user. For example, a school may use a combination of letters from a student's first and last names as a user name. For example, Brittany Stearn's user name might be stearns_brit. Some websites use your email address as the user name. Information technology (IT) departments may assign passwords so that they have a record in case the employee leaves or forgets the password.

With other systems, users select their own user names and/or passwords. Many users select a combination of their first and last names for their user names. Many online social networks, media sharing sites, and retail and other websites allow you to choose your own user name. You might select a name that is formed from parts of your real name or nickname and possibly some numbers, if the name you want is taken (such as britstearns04). If you wish to remain more anonymous, choose a user name that combines common words, or reflects your interests (such as guitarboston27).

Once you select a password, change it frequently. Read Secure IT 1-3 in Chapter 1 for tips about creating strong passwords. Do not disclose your password to anyone or write it on a slip of paper kept near the computer, especially taped to the monitor or under the keyboard. Email and telemarketing scams often ask unsuspecting users to disclose their credit card numbers, so be wary if you did not initiate the inquiry or phone call. Read Secure IT 5-3 for tips about using a password manager.

BTW

Single Sign On

When you enter your user name into a *single sign on* account, such as for Microsoft, Google, Twitter, and Facebook, you automatically are signed in to other accounts and services. Many also recognize your information to provide additional customized content.

SECURE IT 5-3

Safely Use a Password Manager

If you use the same password to access your banking, shopping, online social networks, and school accounts, you are not alone. Many people think one password is sufficient protection for all their vital online accounts, but cyberthieves are aware of this flawed thinking and take advantage of this practice. Security experts recommend using different user names and passwords for every account and changing the passwords frequently.

Keeping track of all these accounts can be an overwhelming task. A *password manager*, also called a *password organizer*, is a convenient service that stores all your account information securely. Once you select a service, you download and install the software and create one master password. The first time you view a password-protected website and enter your user name and password, the password manager saves this information. The next time you visit one of these websites or apps, the software supplies the account information automatically. Password managers use two-step verification and advanced encryption techniques (discussed later in this chapter) to ensure information is stored securely.

Some managers offer the option to generate random passwords, which have a unique combination of jumbled numbers and letters that are difficult for criminals to steal, for each account. Other features include the ability to auto-fill information, such as your name, address, and phone number, on forms and to provide a hint if you have forgotten your master password.

Password manager services can be free to use or may require a small annual fee. Some security experts recommend using a service that charges a fee, stating that these companies may provide more features. Before using any manager, call the company and ask about security measures, the ability to sync with multiple mobile devices, 24-hour customer service via live chat or phone, and limits on the number of passwords that can be saved.

Consider This: Do you use a password manager? If so, do you feel secure storing all your sign in and password information in this service? If not, how do you keep track of your passwords?

CONSIDER THIS

Why do some websites allow you to use your email address as a user name?

No two users can have the same email address; that is, your email address is unique to you. This means you can use your email address and password from one website to validate your identity on another website. Facebook, Google, and Twitter, for example, are three popular websites that provide authentication services to other applications. By using your email address from one of these websites to access other websites, you do not have to create or remember separate user names and passwords for the various websites you visit.

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 grandparent's first name, your favorite food, your first pet's name, or the name of the elementary school you attended. These items should be facts that you easily remember but are not easy for others to discover about you when using a search engine or examining your profiles on online social networks. As with a password, if the user's response does not match information on file, the system denies access.

Passphrase 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 often can be up to 100 characters in length, are more secure than passwords, yet can be easy to remember because they contain words.

PIN A **PIN** (personal identification number), sometimes called a *passcode*, is a numeric password, either assigned by a company or selected by a user. PINs provide an additional level of security. Select PINs carefully and protect them as you do any other password. For example, do not use the same four digits, sequential digits, or dates others could easily determine, such as birth dates.

BTW

Default Passwords

If a program or device has a default or preset password, such as admin, be sure to change it to prevent unauthorized access.

CONSIDER THIS

Why do some websites display distorted characters you must reenter along with your password?

These websites use a CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart. A *CAPTCHA* is a program developed at Carnegie Mellon University that displays an image containing a series of distorted characters for a user to identify and enter in order to verify that user input is from humans and not computer programs (Figure 5-7).

A CAPTCHA is effective in blocking computer-generated attempts to access a website, because it is difficult to write programs for computers to detect distorted characters, while humans generally can recognize them. For visually impaired users or if words are too difficult to read, the CAPTCHA text can be read aloud; you also have the option of generating a new CAPTCHA.

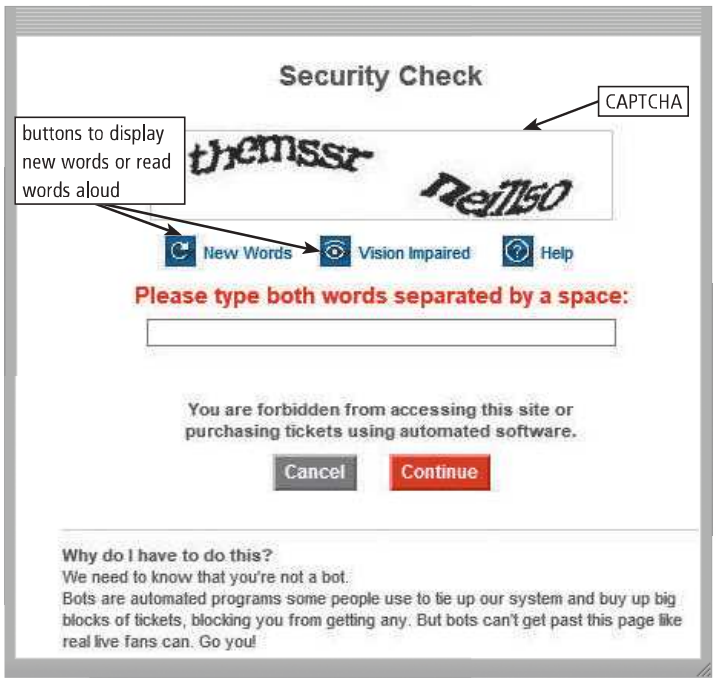


Figure 5-7 To continue with the ticket order process at the Ticketmaster website, the user must enter the characters in the CAPTCHA, which consists of the letters, themssr neillso, in this case.
Source: Carnegie Mellon University

Possessed Objects

A possessed object is any item that you must possess, or carry with you, in order 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 ATM (automated teller machine), for example, is a possessed object that allows access to your bank account.

Biometric Devices

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 a computer or mobile device verifying a physical or behavioral characteristic. If the digital code in the computer or mobile device does not match the personal characteristic code, the computer or mobile device 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, face recognition systems, hand geometry systems, voice verification systems, signature verification systems, iris recognition systems, and retinal scanners.

Fingerprint Reader A **fingerprint reader**, or fingerprint scanner, captures curves and indentations of a fingerprint (Figure 5-8). Organizations use fingerprint readers to secure doors, computers, and software. With the cost of fingerprint readers often less than $100, some home and small business users install fingerprint readers to authenticate users before they can access a personal computer.

Figure 5-8 A fingerprint reader.
© Flynavyjp / Dreamstime.com

The reader also can be set up to perform different functions for different fingers; for example, one finger starts a program and another finger shuts down the computer. External fingerprint readers usually plug into a USB port.

Some laptops, smartphones, and smartwatches have a built fingerprint reader. Using their fingerprint, users can unlock the computer or device, sign in to programs and websites via their fingerprint instead of entering a user name and password, and on some devices, even test their blood pressure and heart rate.

Discover More: Visit this chapter's free resources to learn more about fingerprint readers.

CONSIDER THIS

What is a lock screen?

A *lock screen* is a screen that restricts access to a computer or mobile device until a user performs a certain action. Some simply require a user swipe the screen to unlock the screen. Others verify a user's identity by requiring entry of a password, PIN, or passcode; a fingerprint scan; or a gesture swipe (Figure 5-9). Gestures are motions users make on a touch screen with the tip of one or more fingers or their hand. For example, to unlock the screen on a phone, a user could connect the dots on the screen using a pattern previously defined by the user.

Figure 5-9 Some ways users unlock screens include entering a passcode, scanning a fingerprint, and swiping a gesture.
© iStockPhoto / franckreporter; © Alexey Boldin / Shutterstock; © iStockPhoto / Carpe89

BTW
Technology Trend
Discover More: Visit this chapter's free resources to learn more about uses of face recognition technology.

Face Recognition System A *face recognition system* captures a live face image and compares it with a stored image to determine if the person is a legitimate user. Some buildings use face recognition systems to secure access to rooms. Law enforcement, surveillance systems, and airports use face recognition to protect the public. Some mobile devices use face recognition systems to unlock the device. Face recognition programs are becoming more sophisticated and can recognize people with or without glasses, makeup, or jewelry, and with new hairstyles.

Hand Geometry System A *hand geometry system* measures the shape and size of a person's hand (Figure 5-10). Because hand geometry systems can be expensive, they often are used in larger companies to track workers' time and attendance or as security devices. Colleges use hand geometry systems to verify students' identities. Daycare centers and hospital nurseries use them to identify parents who pick up their children.

Figure 5-10 A hand geometry system verifies identity based on the shape and size of a person's hand.
Courtesy of Ingersoll Rand Security Technologies

Voice Verification System A *voice verification system* compares a person's live speech with their stored voice pattern. Larger organizations sometimes use voice verification systems as time and attendance devices. Many companies also use this technology for access to sensitive files and networks. Some financial services use voice verification systems to secure phone banking transactions.

Signature Verification System A *signature verification system* recognizes the shape of your handwritten signature, as well as measures the pressure exerted and the motion used to write the signature. Signature verification systems use a specialized pen and tablet. Signature verification systems often are used to reduce fraud in financial institutions.

CONSIDER THIS

Do retailers use a signature verification system for credit card purchases?

No. With a credit card purchase, users sign their name on a signature capture pad using a stylus attached to the device. Software then transmits the signature to a central computer, where it is stored. Thus, the retailers use these systems simply to record your signature.

Iris Recognition System
High security areas use iris recognition systems. The camera in an iris recognition system uses iris recognition technology to read patterns in the iris of the eye (Figure 5-11). These patterns are as unique as a fingerprint. Iris recognition systems are quite expensive and are used by government security organizations, the military, and financial institutions that deal with highly sensitive data. Some organizations use retinal scanners, which work similarly but instead scan patterns of blood vessels in the back of the retina.

Figure 5-11 An iris recognition system.

CONSIDER THIS

How popular are biometric devices?
Biometric devices are gaining popularity as a security precaution because they are a virtually foolproof method of identification and authentication. For example, some grocery stores, retail stores, and gas stations 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.

BTW
Two-Step Verification
Users should register a landline phone number, alternate email address, or other form of contact beyond a mobile phone number so that they still can access their accounts even if they lose their mobile phone.

Two-Step Verification

In an attempt to further protect personal data and information from online thieves, many organizations such as financial institutions or universities that store sensitive or confidential items use a two-step verification process. With **two-step verification**, also known as *two-factor verification*, a computer or mobile device uses two separate methods, one after the next, to verify the identity of a user.

ATMs (automated teller machines) usually requires a two-step verification. Users first insert their ATM card into the ATM (Step 1) and then enter a PIN (Step 2) to access their bank account. 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.

Another use of two-step verification requires a mobile phone and a computer. When users sign in to an account on a computer, they enter a user name and a password (Step 1). Next, they are prompted to enter another authentication code (Step 2), which is sent as a text or voice message or via an app on a smartphone (Figure 5-12). This second code generally is valid for a set time, sometimes only for a few hours. If users do not sign in during this time limit, they must repeat the process and request another verification code. Microsoft and Google commonly use two-step verification when you sign in to their websites. If you sign in from a device you use frequently, you can elect to bypass this step.

Internet Research
Which websites use two-step verification?
Search for: two-step verification websites

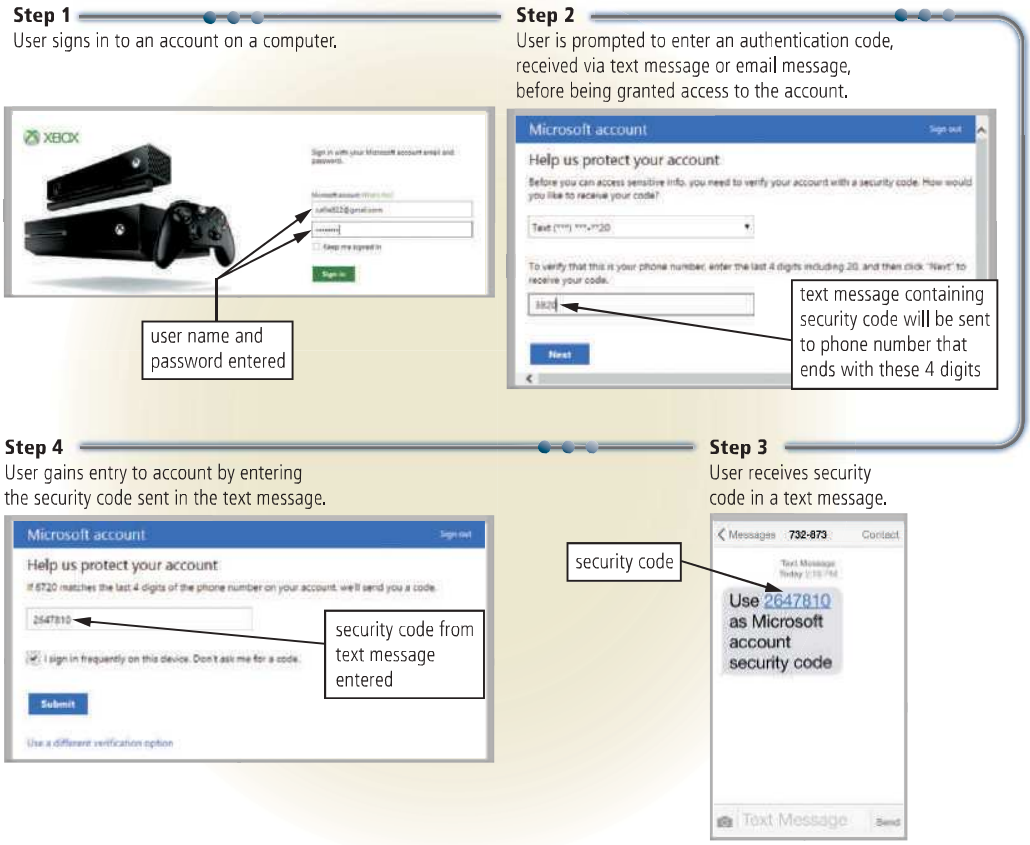


Figure 5-12 This figure shows an example of two-step authentication.
Source: Microsoft

CONSIDER THIS

Can users circumvent the two-step verification process?
Users may be able to specify a computer as a trusted device during a two-step verification so that future sign-in attempts on that same computer will bypass the two-step verification. Only limited-use computers in safe areas should be identified as a trusted device.

Digital Forensics

Digital forensics, also called *cyberforensics*, is the discovery, collection, and analysis of evidence found on computers and networks. Digital forensics involves the examination of media, programs, data and log files on computers, mobile devices, 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.

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.

BTW
High-Tech Talk
Discover More: Visit this chapter's free resources to learn more about digital forensics.

NOW YOU SHOULD KNOW

Be sure you understand the material presented in the sections titled Digital Security Risks, Internet and Network Attacks, and Unauthorized Access and Use, as it relates to the chapter objectives.
Now you should know …

- How cybercriminals' backgrounds and intent vary (Objective 1)
- How you can protect your computers and devices from malware, botnets, DoS attacks, back doors, and spoofing (Objective 2)
- Why you should use a firewall (Objective 2)
- How you can prevent unauthorized users from accessing your home or office computers and devices (Objective 3)

Discover More: Visit this chapter's premium content for practice quiz opportunities.

Software Theft

Software theft occurs when someone steals software media, intentionally erases programs, illegally registers and/or activates a program, or illegally copies a program.

- Physically stealing software: A perpetrator physically steals the media that contains the software, or steals the hardware that contains the media that contains the software. For example, an unscrupulous library patron might steal a game CD/DVD.
- Intentionally erasing software: A perpetrator erases the media that contains the software. For example, a software developer who is terminated from a company may retaliate by removing or disabling the programs he or she has written from company computers.
- Illegal registration/activation: A perpetrator illegally obtains 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.
- Illegal copying: A perpetrator copies software from manufacturers. **Software piracy**, often referred to simply as **piracy**, is the unauthorized and illegal duplication of copyrighted software. Piracy is the most common form of software theft.

BTW
BSA
To promote understanding of software piracy, a number of major worldwide software companies formed the *Business Software Alliance* (*BSA*). The BSA operates a website and antipiracy hotlines around the world.

Safeguards against Software Theft

To protect software media from being stolen, owners should keep original software boxes and media or the online confirmation of purchased software in a secure location, out of sight of prying eyes. All computer users should back up their files and drives regularly, in the event of theft. When some companies terminate a software developer or if the software developer 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.

Many manufacturers incorporate an activation process into their programs to ensure the software is not installed on more computers than legally licensed. During the **product activation**, which is conducted either online or by phone, users provide the software product's identification number to associate the software with the computer or mobile device on which the software is installed. Usually, the software can be run a preset number of times, has limited functionality, or does not function until you activate it.

To further protect themselves from software piracy, software manufacturers issue users license agreements. As discussed in Chapter 4, a **license agreement** is the right to use software. That is, you do not own the software. 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*). The license agreement provides specific conditions for use of the software, which a user must accept before using the software. These terms usually are displayed when you install

Internet Research
What are the penalties for piracy?
Search for: piracy penalties

the software. Use of the software constitutes acceptance of the terms on the user's part. Figure 5-13 identifies the conditions of a typical single-user license agreement.

To support multiple users' access of software, most manufacturers sell network versions or site licenses of their software, which usually costs less than buying individual stand-alone copies of the software for each computer. A *network license* is a legal agreement that allows multiple users to access the software on the server simultaneously. The network license fee usually is based on the number of users or the number of computers attached to the network. A *site license* is a legal agreement that permits users to install the software on multiple computers — usually at a volume discount.

Discover More: Visit this chapter's free resources to learn more about license agreements.

Typical Conditions of a Single-User License Agreement

You can…

- Install the software on only one computer or device. (Some license agreements allow users to install the software on a specified number of computers and/or mobile devices.)
- 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.

You cannot…

- 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.

Figure 5-13 A user must accept the terms of a license agreement before using the software.

CONSIDER THIS

Can you install software on work computers or work-issued smartphones?

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

Information Theft

Information theft occurs when someone steals personal or confidential information. 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 cybercrime. 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.

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

Encryption

Encryption is the process of converting data that is readable by humans into encoded 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 email message. To read the data, the recipient must **decrypt**, or decode it. For example, users may specify that an email application encrypt a message before sending it securely. The recipient's email application would need to decrypt the message in order for the recipient to be able to read it.

BTW
High-Tech Talk
Discover More: Visit this chapter's free resources to learn more about encryption algorithms.

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. A simple encryption algorithm might switch the order of characters or replace characters with other characters. 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 5-14). Public key encryption software generates both the private key and the public key. A message encrypted with a public key can be 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 webpage or a public-key server, or they may be emailed. The private key, by contrast, should be kept confidential.

Some operating systems and email programs allow you to encrypt the contents of files and messages that are stored on your computer. You also can purchase an encryption program to encrypt files. Many browsers use encryption when sending private information, such as credit card numbers, over the Internet.

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 laptop, smartphone, or other mobile device.

Discover More: Visit this chapter's free resources to learn more about encryption algorithms and programs.

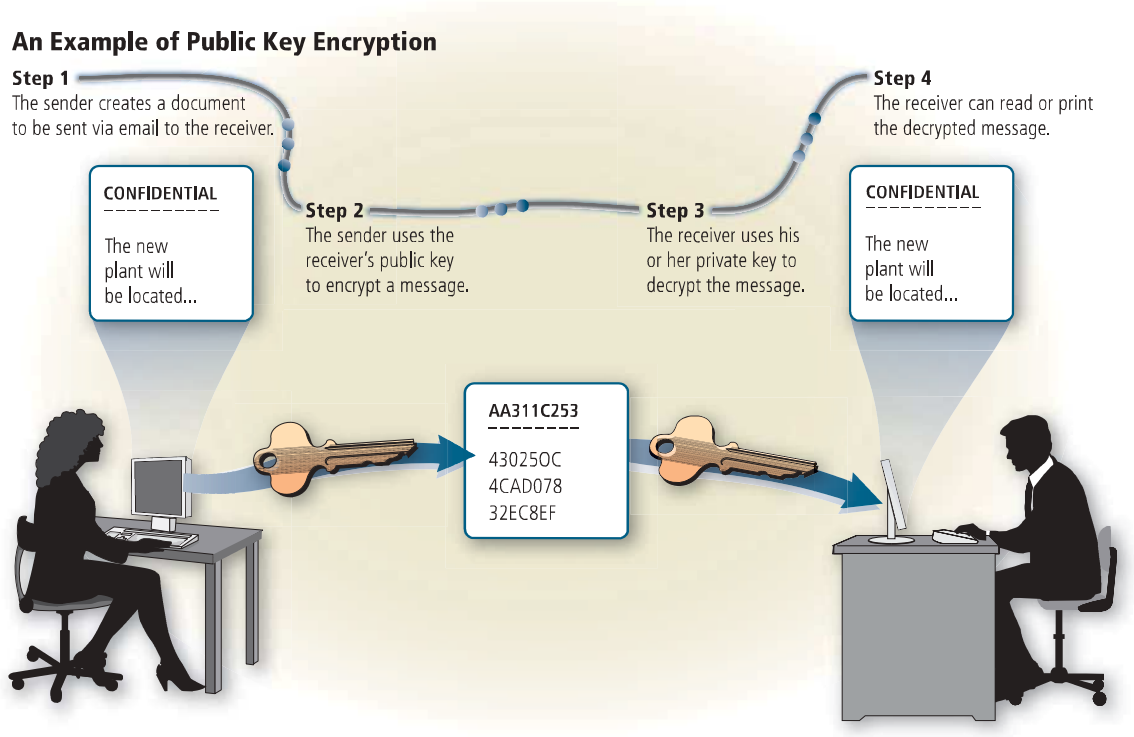


Figure 5-14 This figure shows an example of public key encryption.
© Cengage Learning

Digital Signatures and Certificates

A **digital signature** is an encrypted code that a person, website, or organization attaches to an electronic message to verify the identity of the message sender. Digital signatures often are used to ensure that an impostor is not participating in an Internet transaction. That is, digital signatures can help to prevent email forgery. A digital signature also can verify that the content of a message has not changed.

A **digital certificate** is a notice that guarantees a user or a website is legitimate. E-commerce applications commonly use digital certificates. Browsers often display a warning message if a website does not have a valid digital certificate.

A website that uses encryption techniques to secure its data is known as a **secure site** (Figure 5-15). Web addresses of secure sites often begin with https instead of http. Secure sites typically use digital certificates along with security protocols.

CONSIDER THIS

Who issues digital certificates?

A *certificate authority* (*CA*) is an organization that issues digital certificates. Each CA is a trusted third party that takes responsibility for verifying the sender's identity before issuing a certificate. Individuals and companies can purchase digital certificates from one of more than 35 online CA providers. The cost varies depending on the desired level of data encryption, with the strongest levels recommended for financial and e-commerce transactions.

Discover More: Visit this chapter's free resources to learn more about security protocols, digital certificates and signatures, and CA providers.

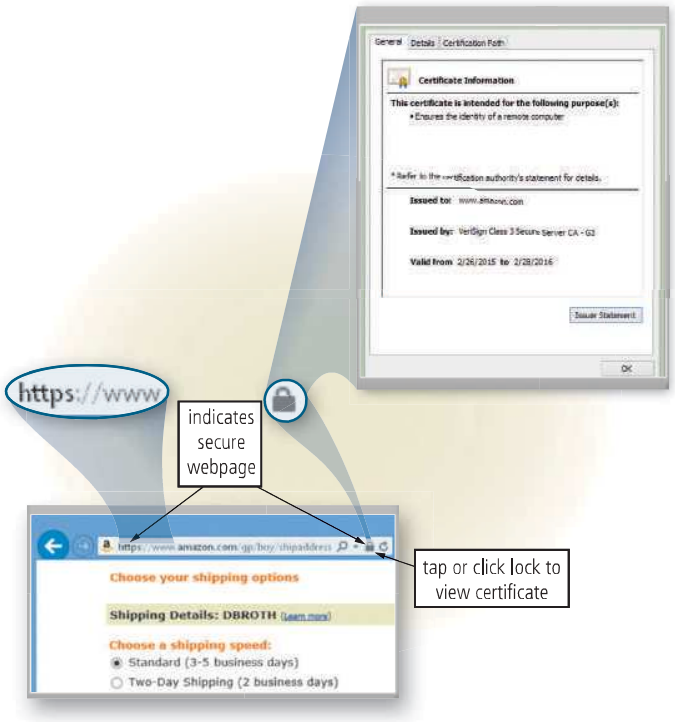


Figure 5-15 Web addresses of secure sites, such as the Amazon.com checkout, often begin with https instead of http. Browsers also often display a lock symbol in the window, which you usually can tap or click to see the associated digital certificate.

Source: Amazon.com and Microsoft

Mini Feature 5-1: Cloud Data Privacy

Privacy and security concerns arise when consumers and businesses consider moving their data to an online storage service. Read Mini Feature 5-1 to learn about privacy issues surrounding cloud data storage. Read Ethics & Issues 5-2 to consider who is responsible for data left on the cloud.

MINI FEATURE 5-1

Cloud Data Privacy

Privacy and security concerns arise when consumers and businesses consider moving their data to an online storage service. While the cloud offers a tremendous amount of storage space at a relatively low cost, the security of data and the reliability of cloud companies trigger concerns.

When people register for a cloud computing service, they sign a written contract or tap or click an online OK or Agree button to affirm they read and understand the terms of the agreement. Any data saved on the cloud is entrusted to the third-party provider, which has a legal obligation to protect the data from security breaches. The company also must guard against data loss due to physical disasters, such as power outages, cooling failures, and fire. When data has been compromised, many states require the company to disclose the issue to the data owner promptly.

The Cloud Security Alliance (CSA) warns of hackers who register for the service with a credit card or for a free trial period and then unleash malware in an attempt to gain access to passwords. Because the registration and validation procedure for accessing the cloud is relatively anonymous, authorities can have difficulty locating the abusers.

Another concern arises when transferring data over a network to the cloud. When the data is traveling to or from a computer and the cloud service, it is subject to interception. To minimize risk, security experts emphasize that the web address of the website you are visiting must begin with https, and the data should be encrypted and authenticated.

Law enforcement's access to the data raises another security issue. Email messages stored on a private server belong to the company or individual who owns the computer, so law enforcement officials must obtain a search warrant to read a particular user's messages. In contrast, law enforcement officials can access email messages stored on the cloud by requesting the information from the company that owns the cloud service. The user might not be notified of the search until up to 90 days after the search occurred; moreover, the search may occur without limitations and may include continuous monitoring of an individual's email communications.

International laws and industry regulations protect sensitive and personal data. Germany has some of the strictest cloud data privacy laws, and, in general, the European Union's privacy regulations are more protective that those in the United States. In much of Europe, for example, consumers must agree to have their personal information collected, and they can review the data for accuracy. The education, health care, and financial services industries in the United States have strict data privacy regulations that affect cloud storage. For example, the Family Educational Rights and Privacy Act (FERPA) regulates the confidentiality of students' educational records, so colleges must obtain students' consent to share data with cloud storage providers and other third parties.

Cloud storage companies have increased their privacy and security features in recent years. Many allow consumers and businesses to protect files with passwords or require two-step authentication to access files, to delete data if a mobile device has been stolen or lost, and to delete data that has been stored past an expiration date.

Discover More: Visit this chapter's free resources to learn more about cloud security breaches, international laws and industry regulations, and protecting online data.

Consider This: How much of your personal data is stored on the cloud? Do you have concerns about the security of this data? Have you ever received a notice that any of your online data has been compromised? Should online social networks or email providers give more explicit notice that data is stored on the cloud? Should law enforcement officials be able to access your data without your consent? Why or why not?

© iStockPhoto / maxkabakov

BTW

Technology Trend

Discover More: Visit this chapter's free resources to learn more about cloud security.

ETHICS & ISSUES 5-2

Who Is Responsible for Data Left on the Cloud?

Businesses often contract with cloud storage providers for data storage. Many businesses also use cloud storage providers to store customer data. This data could include contact information, credit card numbers, and ordering history.

Ownership of cloud data becomes an issue when a cloud storage provider or the business using the cloud services closes. Other issues include what happens if the business fails to pay the cloud storage provider, or when a contract ends. Many feel that it is the responsibility of the business owner to remove and destroy company data before a contract ends. Supporters of this argument believe that cloud storage providers should not be accessing data they host. Others contend that if a business fails to remove and destroy its data before its cloud storage contract ends, cloud storage providers should return the data, or remove the data permanently.

An ongoing debate exists related to who is responsible for cloud data security. Many experts put the responsibility of securing data in the hands of the data owner. Others advocate for a shared security model, in which the cloud storage provider includes security tools, but the company provides additional security as needed.

Ownership and security of data should be included in any contract between a business and cloud storage provider. Contracts also should specify what happens in a variety of scenarios, including if either party stops its operations, or if hackers access the data.

Consider This: If a business stops its operations, who should remove its data from cloud storage? Why? If a customer does not remove its data before a contract ends, should a cloud storage provider return the data, or can it remove or sell the data? Why or why not? Who is responsible for data security? Why?

Hardware Theft, Vandalism, and Failure

Users rely on computers and mobile devices to create, store, and manage important information. As discussed in Chapter 3, you should take measures to protect computers and devices from theft, vandalism, and failure.

Hardware theft is the act of stealing digital equipment. Hardware vandalism involves defacing or destroying digital equipment. Hardware can fail for a variety of reasons: aging hardware, natural or man-made disasters, or random events such as electrical power problems, and even errors in programs or apps. Figure 5-16 summarizes the techniques you can use to safeguard hardware from theft, vandalism, and failure.

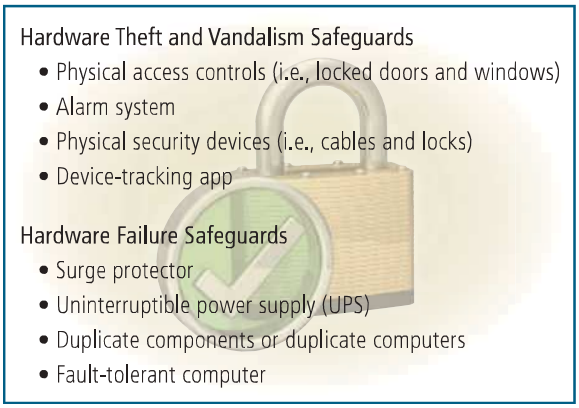


Figure 5-16 Summary of safeguards against hardware theft, vandalism, and failure.

Backing Up — The Ultimate Safeguard

To protect against data loss caused by hardware/software/information theft or system failure, users should back up computer and mobile device files regularly. As previously described, a **backup** is a duplicate of a file, program, or media that can be used if the original is lost, damaged, or destroyed; and 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 or mobile device.

If you choose to back up locally, be sure to use high-quality media. A good choice for a home user might be optical discs or an external hard drive. Keep your backup media in a fireproof and heat-proof safe or vault, or offsite. *Off-site* means in a location separate from where you typically store or use your computer or mobile device. Keeping backup copies off-site minimizes the chance that a single disaster, such as a fire, would destroy both the original and the backup media. An off-site location can be a safe deposit box at a bank, a briefcase, or cloud storage or cloud backup.

Cloud storage provides storage to customers, usually along with synchronization services but often on smaller amounts of data. By contrast, cloud backup provides only backup and retrieval services, but generally provides continuous data protection (discussed next) to the cloud. More customers are opting for cloud backup because it saves them the cost of maintaining hardware (Figure 5-17).

BTW

Technology Innovator

Discover More: Visit this chapter's free resources to learn about the device-tracking app, LoJack.

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 tools exist. Cloud storage providers may offer backup services. Users of a cloud backup service install software on their computers that backs up files to the cloud as they are modified.

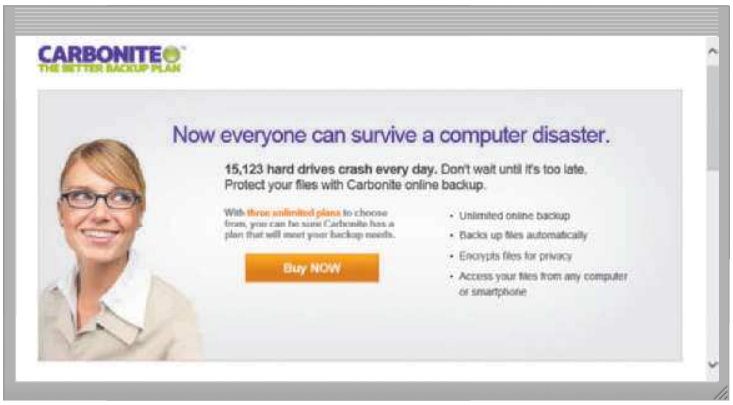


Figure 5-17 Cloud storage, such as Carbonite shown here, is a popular method for off-site backups.
Source: Carbonite, Inc.

Business and home users can perform four types of backup: full, differential, incremental, or selective. A fifth type, continuous data protection, often is used only by large enterprises to back up data to an in-house network storage device purchased and maintained by the enterprise. Cloud backup services, a sixth option, are providing continuous data protection capabilities at a lower cost. Table 5-2 summarizes the purpose, advantages, and disadvantages of each of these backup methods.

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. When a new backup is performed, the child becomes the parent, the parent becomes the grandparent, and the media on which the grandparent copy was stored may be erased and reused for a future backup.

Table 5-2 Various Backup Methods

Type of Backup	Description	Advantages	Disadvantages
Full backup	Copies all of the files on media in the computer.	Fastest recovery method. All files are saved.	Longest backup time.
Differential backup	Copies only the files that have changed since the last full backup.	Fast backup method. Requires minimal storage space to back up.	Recovery is time-consuming because the last full backup plus the differential backup are needed.
Incremental backup	Copies only the files that have changed since the last full or incremental backup.	Fastest backup method. Requires minimal storage space to back up. Only most recent changes saved.	Recovery is most time-consuming because the last full backup and all incremental backups since the last full backup are needed.
Selective backup	Users choose which folders and files to include in a backup.	Fast backup method. Provides great flexibility.	Difficult to manage individual file backups. Least manageable of all the backup methods.
Continuous data protection (CDP)	All data is backed up whenever a change is made.	The only real-time backup. Very fast recovery of data.	Very expensive and requires a great amount of storage.
Cloud backup	Files are backed up to the cloud as they change.	Cloud backup provider maintains backup hardware. Files may be retrieved from anywhere with an Internet connection on any device.	Requires an Internet connection, otherwise files are marked for backup when the computer goes back online.

Mini Feature 5-2: Disaster Recovery

A **disaster recovery plan** is a written plan that describes the steps an organization would take to restore its computer operations in the event of a disaster. Read Mini Feature 5-2 to learn about steps an organization takes in the event of a disaster.

MINI FEATURE 5-2

Disaster Recovery

A disaster can be natural or man-made (hackers, viruses, etc.). Each company and each department or division within an organization usually has its own disaster recovery plan. The following scenario illustrates how an organization might implement a disaster recovery plan.

Rosewood Associates is a consulting firm that helps clients use social media for marketing and customer outreach. Last week, a fire broke out in the office suite above Rosewood. The heat and smoke, along with water from the sprinkler system, caused extensive damage. As a result, Rosewood must replace all computers, servers, and storage devices. Also, the company lost all of the data it had not backed up.

Rosewood currently backs up its systems daily to an internal server and weekly to a remote cloud server. Because of damage to the internal server, the company lost several days of data. Rosewood does not have a plan for replacing hardware. Thus, they will lose several additional days of productivity while purchasing, installing, and configuring new hardware.

To minimize the chance of this type of loss in the future, the company hired you as a consultant to help create a disaster recovery plan. You first discuss the types of disasters that can strike, as shown in the table. You then explain that the goal of a disaster recovery plan is to prevent, detect, and correct system threats, and to restore the most critical systems first.

A disaster recovery plan typically contains these four components: emergency plan, backup plan, recovery plan, and test plan.

Emergency Plan: An emergency plan specifies the steps Rosewood will take as soon as a disaster strikes. The emergency plan is organized by type of disaster, such as fire, flood, or earthquake, and includes:

1. Names and phone numbers of people and organizations to notify (company management, fire and police department, clients, etc.)
2. Computer equipment procedures, such as equipment or power shutoff, and file removal; employees should follow these procedures only if it is safe to do so
3. Employee evacuation procedures
4. Return procedures (who can enter the facility and what actions they are to perform)

Backup Plan: The backup plan specifies how Rosewood will use backup files and equipment to resume computer operations, and includes:

1. The location of backup data, supplies, and equipment
2. Who is responsible for gathering backup resources and transporting them to an alternate computer facility
3. The methods by which data will be restored from cloud storage
4. A schedule indicating the order and approximate time each application should be up and running

Considerations for Disaster Recovery

Disaster Type	What to Do First	What Might Occur	What to Include in the Plan
Natural (earthquake, hurricane, tornado, etc.)	Shut off power Evacuate, if necessary Pay attention to advisories Do not use phone lines if lightning occurs	Power outage Phone lines down Structural damage to building Road closings, transportation interruptions Flooding Equipment damage	Generator Satellite phone, list of employee phone numbers Alternate worksite Action to be taken if employees are not able to come to work/leave the office Wet/dry vacuums Make and model numbers and vendor information to get replacements
Man-made (hazardous material spill, terrorist attacks, fire, hackers, malware, etc.)	Notify authorities (fire departments, etc.) of immediate threat Attempt to suppress fire or contain spill, if safe to do so Evacuate, if necessary	Data loss Dangerous conditions for employees Criminal activity, such as data hacking and identity theft Equipment damage	Backup data at protected site Protective equipment and an evacuation plan Contact law enforcement Make and model numbers and vendor information to obtain replacements

Recovery Plan: The recovery plan specifies the actions Rosewood will take to restore full computer operations. As with the emergency plan, the recovery plan differs for each type of disaster. You recommend that Rosewood set up planning committees. Each committee would be responsible for different forms of recovery, such as replacing hardware or software.

Test Plan: The test plan includes simulating various levels of disasters and recording Rosewood's ability to recover. You run a test in which the employees follow the steps in the disaster recovery plan. The test uncovers a few needed recovery actions not specified in the plan, so you modify the plan. A few days later, you run another test without giving the employees any advance notice to test the plan again.

Discover More: Visit this chapter's free resources to learn more about lost productivity, backup plans, and alternate computer facilities.

Consider This: For what kinds of natural and man-made disasters should a company plan? What roles can cloud storage providers play in helping to recover from a disaster? How involved should employees be in developing and testing disaster recovery plans?

Figure 5-18 Wireless access points or routers around campus allow students to access the school network wirelessly from their classrooms, the library, dorms, and other campus locations.

Wireless Security

Billions of home and business users have laptops, smartphones, and other mobile devices to access the Internet, send email and Internet messages, chat online, or share network connections — all wirelessly. 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 (Figure 5-18).

Although wireless access provides many conveniences to users, it also poses additional security risks. Some perpetrators connect to other's wireless networks to gain free Internet access; others may try to access an organization's confidential data.

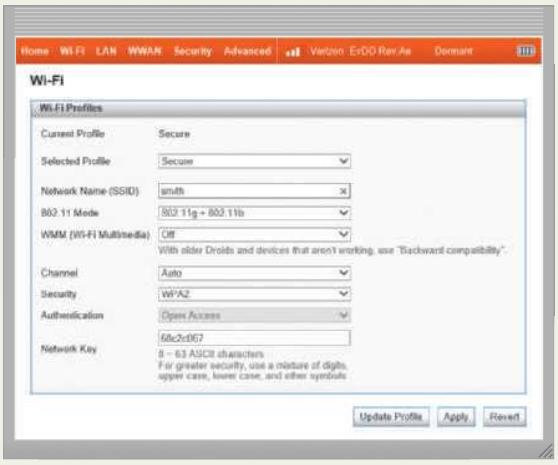
To access a wireless network, the individual must be in range of the wireless network. Some intruders intercept and monitor communications as they transmit through the air. Others connect to a network through an unsecured wireless access point (WAP) or combination router/WAP. Read How To 5-3 for instructions about ways to secure a wireless network, in addition to using firewalls.

HOW TO 5-3

Secure Your Wireless Network

When you set up a wireless network, it is important to secure the network so that only your computers and mobile devices can connect to it. Unsecured wireless networks can be seen and accessed by neighbors and others nearby, which may make it easier for them to connect to and access the data on the computers and mobile devices on your network. The following list provides suggestions for securing your wireless network.

- Immediately upon connecting your wireless access point and/or router, change the password required to access administrative features. If the password remains at its default setting, others may possibly be able to connect to and configure your wireless network settings.
- Change the *SSID* (service set identifier), which is a network name, from the default to something that uniquely identifies your network, especially if you live in close proximity to other wireless networks.
- Do not broadcast the SSID. This will make it more difficult for others to detect your wireless network. When you want to connect a computer or mobile device to your wireless network, it will be necessary to enter the SSID manually.
- Enable an encryption method such as WPA2 (Wi-Fi Protected Access 2), and specify a password or passphrase that is difficult for others to guess. The most secure passwords and passphrases contain more than eight characters, uppercase and lowercase letters, numbers, and special characters.
- Enable and configure the MAC (Media Access Control) address control feature. A *MAC address* is a unique hardware identifier for your computer or device. The *MAC address control* feature specifies the computers and mobile devices that can connect to your network. If a computer or device is not specified, it will not be able to connect.
- Choose a secure location for your wireless router so that unauthorized people cannot access it. Someone who has physical access to a wireless router can restore factory defaults and erase your settings.



Source: Verizon Wireless

Consider This: In addition to safeguarding the data and information on your computers from others, why else might it be a good idea to secure your wireless network?

CONSIDER THIS

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

If you notice the speed of your wireless 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.

Mini Feature 5-3: Mobile Security

As the number of smartphones and mobile devices in use increases, the possibility of security breaches and lost devices increases proportionally. Read Mini Feature 5-3 to learn about ways you can protect sensitive and personal data on your mobile devices.

MINI FEATURE 5-3

Mobile Security

The consequences of losing a smartphone or mobile device are significant given the amount of storage and the variety of personal and business data stored. Symantec, one the world's leading online security companies, projects that only one-half of lost or stolen phones eventually will be returned to their owners. Chances are that the people who find the missing phones likely will have viewed much of the content on the devices in a quest to find the owners and possibly to gain access to private information.

The goal, therefore, for mobile device users is to make their data as secure as possible. Follow these steps to protect sensitive and personal data and to fight mobile cybercrime.

- **Be extra cautious locating and downloading apps.** Any device that connects to the Internet is susceptible to mobile malware. Cyberthieves target apps on widely used phones and tablets. Popular games are likely candidates to house malware, and it often is difficult to distinguish the legitimate apps from the fake apps. Obtain mobile device apps from well-known stores, and before downloading anything, read the descriptions and reviews. Look for misspellings and awkward sentence structure, which could be clues that the app is fake. If something looks awry, do not download. Scrutinize the number and types of permissions the app is requesting. If the list seems unreasonable in length or in the personal information needed, deny permission and uninstall the app.
- **Use a PIN.** Enable the passcode feature on a mobile device as the first step in stopping prying eyes from viewing contents. This four-to-eight-digit code adds a layer of protection. Only emergency functions can be accessed without entering the correct sequence of numbers. This strong code should not be information easily guessed, such as a birthdate.
- **Turn off GPS tracking.** GPS technology can track the mobile device's location as long as it is transmitting and receiving signals to and from satellites. This feature is helpful to obtain directions from your current location, view local news and weather reports, find a lost device, summon emergency personnel, and locate missing children. Serious privacy concerns can arise, however, when the technology is used in malicious ways, such as to stalk individuals or trace their whereabouts. Unless you want to allow others to follow your locations throughout the day, disable the GPS tracking feature until needed.
- **Use mobile security software.** Protection is necessary to stop viruses and spyware and to safeguard personal and business data. Mobile security apps can allow you to lock your mobile device and SIM card remotely, erase the

(*Continued*)

memory, and activate the GPS function. Other apps prevent cyberthieves from hijacking your phone and taking pictures, making recordings, placing calls to fee-imposed businesses, and sending infected messages to all individuals in your contact list. Look for security software that can back up data to a cloud account, set off a screeching alarm on the lost or stolen mobile device, offer live customer service, and provide theft, spam, virus, and malware protection.

- **Avoid tapping or clicking unsafe links.** Tapping or clicking an unknown link can lead to malicious websites. If you receive a text message from someone you do not know or an invitation to tap or click a link, resist the urge to fulfill the request. Your financial institution never will send you a message requesting you to enter your account user name and password. Malicious links can inject malware on the mobile device to steal personal information or to create toll fraud, which secretly contacts wireless messaging services that impose steep fees on a monthly bill.

Discover More: Visit this chapter's free resources to learn more about methods to protect your mobile device and personal information.

Consider This: As the number of smartphones and mobile devices in use increases, the possibility of security breaches and lost devices increases proportionally. How can manufacturers and wireless carriers emphasize the importance of mobile security and convince users to take the precautions suggested in this mini feature? What mobile security safeguards have you taken to protect your smartphone or mobile device? What steps will you take after reading this mini feature?

NOW YOU SHOULD KNOW

Be sure you understand the material presented in the sections titled Software Theft; Information Theft; Hardware Theft, Vandalism, and Failure; Backing Up – The Ultimate Safeguard; and Wireless Security as it relates to the chapter objectives.

Now you should know …

- What actions you are allowed according to a software license agreement (Objective 4)
- Why you would want to use encryption, digital signatures, or digital certificates (Objective 5)
- How you can protect your hardware from theft, vandalism, and failure (Objective 6)
- Which backup method is most suited to your needs (Objective 7)
- How you can protect your wireless communications (Objective 8)

Discover More: Visit this chapter's premium content for practice quiz opportunities.

Ethics and Society

As with any powerful technology, computers and mobile devices can be used for both good and bad intentions. The standards that determine whether an action is good or bad are known as ethics.

Technology ethics are the moral guidelines that govern the use of computers, mobile devices, information systems, and related technologies. Frequently discussed areas of computer ethics are unauthorized use of computers, mobile devices, and networks; software theft (piracy); information accuracy; intellectual property rights; codes of conduct; green computing; and information privacy. The questionnaire in Figure 5-19 raises issues in each of these areas.

Previous sections in this chapter discussed unauthorized use of computers, mobile devices and networks, and software theft (piracy). The following sections discuss issues related to information accuracy, intellectual property rights, codes of conduct, green computing, and information privacy.

Your Thoughts?

		Ethical	Unethical
1.	An organization requires employees to wear badges that track their whereabouts while at work.	☐	☐
2.	A supervisor reads an employee's email message.	☐	☐
3.	An employee uses his computer at work to send email messages to a friend.	☐	☐
4.	An employee sends an email message to several coworkers and blind copies his supervisor.	☐	☐
5.	An employee forwards an email message to a third party without permission from the sender.	☐	☐
6.	An employee uses her computer at work to complete a homework assignment for school.	☐	☐
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.	☐	☐
8.	A student copies text from the web and uses it in a research paper for his English Composition class.	☐	☐
9.	An employee sends political campaign material to individuals on her employer's mailing list.	☐	☐
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 grades to be posted online.	☐	☐
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.	☐	☐
12.	An employee who has been laid off installs a computer virus on his employer's computer.	☐	☐
13.	A person designing a webpage finds one on the web similar to his requirements, copies it, modifies it, and publishes it as his own webpage.	☐	☐
14.	A student researches using only the web to write a report.	☐	☐
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.	☐	☐
16.	Someone copies a well-known novel to the web and encourages others to read it.	☐	☐
17.	A person accesses an organization's network and reports to the organization any vulnerabilities discovered.	☐	☐
18.	Your friend uses a neighbor's wireless network to connect to the Internet and check email.	☐	☐
19.	A company uses recycled paper to print a 50-page employee benefits manual that is distributed to 425 employees.	☐	☐
20.	An employee is fired based on the content of posts on his or her online social network.	☐	☐

Figure 5-19 Indicate whether you think the situation described is ethical or unethical. Be prepared to discuss your answers.

Information Accuracy

Information accuracy is a concern today 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 discussed in Chapter 2, users should evaluate the value of a webpage before relying on its content. Be aware that the organization providing access to the information may not be the creator of the information. Read Secure IT 5-4 to consider the risks associated with inaccurate data.

SECURE IT 5-4

Risks Associated with Inaccurate Data

Mapping and navigation software is invaluable for locating unfamiliar destinations. Problems arise, however, when satellite images are outdated or when the desired address cannot be found on a map. Inaccurate data can result in lost revenues for businesses when potential customers cannot find the storefront. It also has caused accidents when drivers followed turn-by-turn GPS directions and drove the wrong way on one-way streets, made illegal turns, or ended at ponds where a road stopped.

Business owners can report incorrect address data to some mapping services. They can, for example, state that the satellite image needs updating, their address has changed, the directions are incorrect, or the street names are inaccurate. In some cases, the maps and addresses are updated quickly, often within a day.

Data entry errors also can lead to lost business, lawsuits, and expenses. In an extreme example, a $125 million Mars Climate Orbiter spacecraft was lost in space because Lockheed Martin engineers performed calculations using English units (pounds) to fire the thrusters guiding the spacecraft, but NASA engineers assumed the data was in metric units (Newtons) and sent the spacecraft 60 miles off course. In another unit conversion error, an axle broke on a Space Mountain roller coaster car at Tokyo Disneyland because it was the wrong size; the error occurred when engineers performed calculations to convert the original Space Mountain master plan from English units to metric units.

In the business world, mistakes can occur when software has not been updated or when employees are overworked, distracted, or faced with repetitive tasks. Software should have safeguards to verify valid data has been entered, such as checking that phone numbers have 10 numeric characters. Data cleaning software can eliminate duplicate database records, locate missing data, and correct discrepancies.

Consider This: Have you ever used a mapping app or website and encountered incorrect information? Would you consider notifying mapping companies of errors in their satellite images or directions? What steps can companies take to help employees enter data accurately?

Figure 5-20 This digitally edited photo shows a fruit that looks like an apple on the outside and an orange on the inside.

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 graphic output, such as a retouched photo. With graphics equipment and software, users easily can digitize photos and then add, change (Figure 5-20), or remove images.

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 and easily can be redistributed or altered without the creator's permission.

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

A common infringement of copyright is piracy, where people 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 website, 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 on 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 take term papers they have written and post them 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.

Internet Research
What is meant by fair use?
Search for: fair use definition

Internet Research
What is creative commons?
Search for: creative commons

Codes of Conduct

A **code of conduct** is a written guideline that helps determine whether a specification is ethical/unethical or allowed/not allowed. An IT code of conduct focuses on acceptable use of technology. Employers and schools often specify standards for the ethical use of technology in an IT code of conduct and then distribute these standards to employees and students (Figure 5-21). You also may find codes of conduct online that define acceptable forms of communications for websites where users post commentary or other communications, such as blogs, wikis, online discussions, and so on.

Sample IT Code of Conduct

1. Technology may not be used to harm other people.
2. Employees may not meddle in others' files.
3. Employees may use technology only for purposes in which they have been authorized.
4. Technology may not be used to steal.
5. Technology may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' technology 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 technology in a way that demonstrates consideration and respect for fellow humans.

Figure 5-21 Sample IT code of conduct employers may distribute to employees.

Green Computing

People use, and often waste, resources such as electricity and paper while using technology. Recall from Chapter 1 that **green computing** involves reducing the electricity and environmental waste while using computers, mobile devices, and related technologies. Figure 5-22 summarizes measures users can take to contribute to green computing.

Personal computers, displays, printers, and other devices 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. 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 (shown in Figure 5-22).

Green Computing Tips

1. Conserve Energy
   a. Use computers and devices that comply with the ENERGY STAR program.
   b. Do not leave a computer or device running overnight.
   c. Turn off the monitor, printer, and other devices when not in use.
2. Reduce Environmental Waste
   a. Use paperless methods to communicate.
   b. Recycle paper and buy recycled paper.
   c. Recycle toner and ink cartridges, computers, mobile devices, printers, and other devices.
   d. Telecommute.
   e. Use videoconferencing and VoIP for meetings.

Figure 5-22 A list of suggestions to make computing healthy for the environment.

Enterprise data centers and computer facilities consume large amounts of electricity from computer hardware and associated devices 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.
- Purchase high-efficiency equipment.
- Use sleep modes and other power management features for computers and devices.
- Buy computers and devices with low power consumption processors and power supplies.
- When possible, use outside air to cool the data center or computer facility.

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 and devices.

Internet Research
Where can I recycle outdated electronics?
Search for: recycle old electronics

CONSIDER THIS

Should you save out-of-date computers and devices?

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. Before recycling, refurbishing, or discarding your old computer, be sure to erase, remove, or destroy its hard drive so that the information it stored remains private.

Discover More: Visit this chapter's free resources to learn more about the ENERGY STAR program.

How to Safeguard Personal Information

1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your phone number or Social Security number on personal checks.
3. Have an unlisted or unpublished phone number.
4. If you have Caller ID, find out how to block your number from displaying on the receiver's system.
5. Do not write your phone number on charge or credit receipts.
6. Ask merchants not to write credit card numbers, phone 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 websites. 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 email account. Use this email address for merchant forms.
18. Turn off file and printer sharing on your Internet connection.
19. Install a personal firewall.
20. Sign up for email filtering through your ISP or use an anti-spam program.
21. Do not reply to spam for any reason.
22. Surf the web anonymously or through an anonymous website.

Figure 5-23 Techniques to keep personal data private.

Information Privacy

Information privacy refers to the right of individuals and companies to deny or restrict the collection, use, and dissemination of information about them. Organizations often use huge databases to store records, such as employee records, medical records, financial records, and more. 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. Websites often collect data about you, so that they can customize advertisements and send you personalized email messages. Some employers monitor your computer usage and email messages.

Figure 5-23 lists measures you can take to make your personal data more private. The following sections address techniques companies and employers use to collect your personal data.

Discover More: Visit this chapter's free resources to learn more about your credit report.

Electronic Profiles

When you fill out a printed form, such as a magazine subscription or contest entry, or an online form to sign up for a service, create a profile on an online social network, or register a product warranty, the merchant that receives the form usually stores the information you provide in a database. Likewise, every time you tap or click an advertisement on the web or perform a search online, your information and preferences enter a database. Some merchants may sell or share the contents of their databases with national marketing firms and Internet advertising firms. By combining this data with information from public records, such as driver's licenses and vehicle registrations, these firms can create an electronic profile of individuals. Electronic profiles may

include personal details, such as your age, address, phone number, marital status, number and ages of dependents, interests, and spending habits.

Direct marketing supporters claim 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 argue 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 websites allow people to specify whether they want their personal information shared or preferences retained (Figure 5-24).

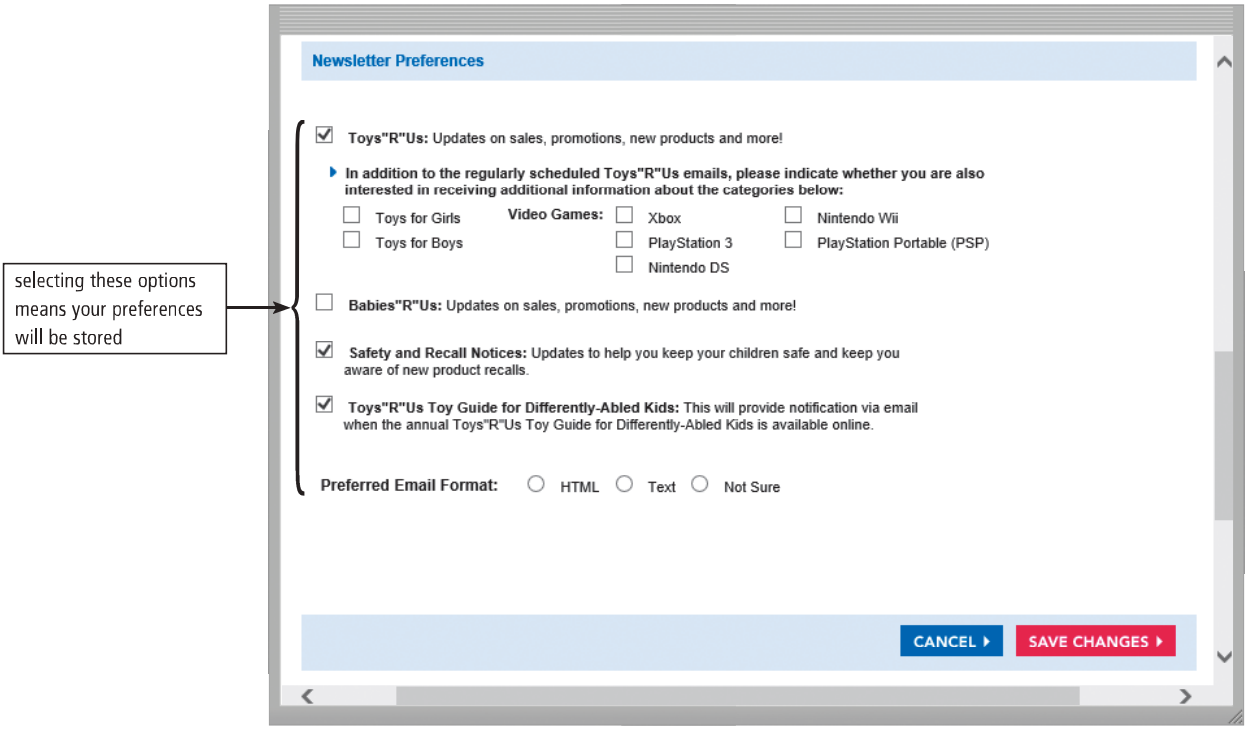


Figure 5-24 Many companies, such as Toys"R"Us shown here, allow users to specify whether they want the company to retain their preferences.
Source: Geoffrey, LLC

Cookies

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, postal code, or viewing preferences. Websites use cookies for a variety of purposes:

- Most websites that allow for personalization use cookies to track user preferences. These cookies may obtain their values when a user fills in an online form requesting personal information. Some websites, for example, store user names in cookies in order to display a personalized greeting that welcomes the user, by name, back to the website. Other websites allow users to customize their viewing experience with preferences, such as local news headlines, the local weather forecast, or stock quotes.
- Some websites use cookies to store user names and/or passwords, so that users do not need to enter this information every time they sign in to the website.
- 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 websites use cookies to track how often users visit a site and the webpages they visit while at the website.
- Websites may use cookies to target advertisements. These websites store a user's interests and browsing habits in the cookie.

CONSIDER THIS

Do websites ever sell information stored in cookies?

Some websites sell or trade information stored in your cookies to advertisers — a practice many believe to be unethical. If you do not want personal information distributed, you should limit the amount of information you provide to a website or adjust how your browser handles cookies. You can regularly clear cookies or set your browser to accept cookies automatically, prompt if you want to accept a cookie, or disable all cookie use. Keep in mind if you disable cookie use, you may not be able to use some e-commerce websites. As an alternative, you can purchase software that selectively blocks cookies.

Many commercial websites send a cookie to your browser; your computer's hard drive then stores the cookie. The next time you visit the website, your browser retrieves the cookie from your hard drive and sends the data in the cookie to the website. Figure 5-25 illustrates how websites work with cookies. A website can read data only from its own cookie file stored on your hard drive. That is, it cannot access or view any other data on your hard drive — including another cookie file.

Figure 5-25 This figure shows how cookies work.

Phishing

Recall from Chapter 4 that **phishing** is a scam in which a perpetrator sends an official looking email message that attempts to obtain your personal and/or financial information. These messages look legitimate and request that you update credit card numbers, Social Security numbers, bank account numbers, passwords, or other private information. Read How To 5-4 for instructions about protecting yourself from phishing scams.

HOW TO 5-4

Protect against a Phishing Scam

Phishing scams can be perpetrated via email messages, websites, and even on the phone. The following guidelines will help protect you against a phishing scam.

Phone Scams

- If you receive a phone call from someone claiming to be from a company with which you do business, record his or her name and the time of the call. Do not disclose personal or financial information to the caller. If the caller is offering a product or service and is requesting a payment, call the company back at the number you have on file, and ask to be transferred to the person who called you initially.
- Whenever possible, enter your payment information on secure websites instead of reading credit card numbers or bank account information on the phone. You never know whether the caller is recording your payment information to use later for malicious purposes.

Email Scams

- If you receive an email message from someone requesting you to verify online account or financial information, do not reply with this information.
- Never tap or click links in email messages, even if the message appears to be from someone you know. Nor should you copy and paste the link from the email message to a browser. Instead, type the link's web address into a browser's address bar manually, and make sure you type it correctly. If you are visiting your financial institution's website, make sure the web address you enter matches the web address you have on file for them.
- Do not reply to email messages asking you for financial assistance — even if the email message appears to originate from someone you know. If you receive this type of email message from someone you know, call the person to verify the message's authenticity.

Website Scams

- When visiting a website, such as your financial institution's website, that will require you to enter confidential information, be sure to type the web address correctly. Typing it incorrectly may take you to a phishing website where the information you enter can be collected by an unknown party.
- Make sure websites requiring your confidential information use the https://protocol.
- Websites with misspellings, poor grammar, or formatting problems may indicate a phishing website. Do not enter personal or financial information on a website that looks suspicious.
- Enable the *phishing filter* in your browser that can warn or block you from potentially fraudulent or suspicious websites.

Consider This: Have you experienced a phishing scam? If so, how did it attempt to trick you into providing personal or financial information? How did you respond?

Clickjacking is yet another similar scam. With *clickjacking*, an object that can be tapped or clicked — such as a button, image, or link — on a website, pop-up ad, pop-under ad, or in an email message or text message contains a malicious program. When a user taps or clicks the disguised object, a variety of nefarious events may occur. For example, the user may be redirected to a phony website that requests personal information, or a virus may download to the computer or mobile device. Browsers typically include clickjacking protection.

Internet Research
Which phishing scams are prevalent?
Search for: recent phishing scams

Spyware and Adware

Recall from Chapter 4 that **spyware** is a program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online. 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. Spyware can enter your computer when you install a new program, through malware, or through a graphic on a webpage or in an email message.

Adware is a program that displays an online advertisement in a banner, a pop-up window, or pop-under window on webpages, email messages, or other Internet services. Adware on mobile phones is known as *madware*, for mobile adware. Sometimes, spyware is hidden in adware.

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

Social Engineering

As related to the use of technology, **social engineering** is defined as gaining unauthorized access to 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 phone, 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 phone numbers or using ATMs, and snoop around computers or mobile devices looking for openly displayed confidential information.

To protect yourself from social engineering scams, follow these tips:

- Verify the identity of any person or organization requesting personal or confidential information.
- When relaying personal or confidential information, ensure that only authorized people can hear your conversation.
- When personal or confidential information appears on a computer or mobile device, ensure that only authorized people can see your screen.
- Shred all sensitive or confidential documents.
- After using a public computer, clear the cache in its browser.
- Avoid using public computers to conduct banking or other sensitive transactions.

Privacy Laws

The concern about privacy has led to the enactment of federal and state laws regarding the storage and disclosure of personal data, some of which are shown in Table 5-3. Common points in some of these laws are as follows:

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 protect the data so that only those employees within the organization who need access to it to perform their job duties have access to it.
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.

Read Ethics & Issues 5-3 to consider the legal issues surrounding your digital footprint.

Table 5-3 Major U.S. Government Laws Concerning Privacy

Law	Purpose
Children's Internet Protection Act	Protects minors from inappropriate content when accessing the Internet in schools and libraries
Children's Online Privacy Protection Act (COPPA)	Requires websites to protect personal information of children under 13 years of age
Computer Abuse Amendments Act	Outlaws transmission of harmful computer code such as viruses
Digital Millennium Copyright Act (DMCA)	Makes it illegal to circumvent antipiracy schemes in commercial software; outlaws sale of devices that copy software illegally
Electronic Communications Privacy Act (ECPA)	Provides the same right of privacy protection of the postal delivery service and phone companies to various forms of electronic communications, such as voice mail, email, and mobile phones
Financial Modernization Act	Protects consumers from disclosure of their personal financial information and requires institutions to alert customers of information disclosure policies
Freedom of Information Act (FOIA)	Enables public access to most government records
HIPAA (Health Insurance Portability and Accountability Act)	Protects individuals against the wrongful disclosure of their health information
PATRIOT (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism)	Gives law enforcement the right to monitor people's activities, including web and email habits
Privacy Act	Forbids federal agencies from allowing information to be used for a reason other than that for which it was collected

Discover More: Visit this chapter's free resources to learn about more privacy laws.

ETHICS & ISSUES 5-3

Do You Have the Right to Be Digitally Forgotten?

Privacy experts, such as The Institute for Responsible Online and Cell-Phone Communication (IROC2), warn that "Your digital activity is public and permanent" and is available permanently to anyone using a search engine. Does it have to be? Do you have a "right to be forgotten" as was ruled by a court in the European Union recently?

In this case, the court ordered a popular search engine to remove links to information that was "inadequate, irrelevant, or no longer relevant." The content in question included many factual articles published by a major news source. Examples included stories about a university student arrested for driving while intoxicated and a referee who lied about a mistake. Free speech advocates criticize the law. They state that a government should not be able to deny access to accurate information. Others argue that a person should be able to request removal of information that is damaging to his or her reputation. Some are concerned that negative incidents may be necessary information for an employer to know about a job seeker, or for those considering a relationship with another person. You can never truly delete your digital footprint because everything you do online has the potential to be forwarded, captured as a screenshot, or archived in databases.

Among the debated issues is whether the rights of a private citizen should differ from those of a public figure. Many argue that different rules apply for celebrities, politicians, and others who choose such professions. Some feel that the responsibility rests on search engines to provide methods that enable individuals to comment on, explain, or select what information is displayed when they are the subject of an Internet search. For example, Google developed the Google Inactive Account Manager, where you can specify what happens to your data after a period of inactivity.

Consider This: Does a government have a right to legislate search engine links? Why or why not? In what, if any, situations should individuals be able to request removal of digital content? Should search engines provide users with tools to control what information about them appears? Why or why not?

Employee Monitoring

Employee monitoring involves the use of computers, mobile devices, or cameras to observe, record, and review an employee's use of a technology, including communications such as email messages, keyboard activity (used to measure productivity), and websites visited. Many programs exist that easily allow employers to monitor employees. Further, it is legal for employers to use these programs.

CONSIDER THIS

Do employers have the right to read employee email messages?

Actual policies vary widely. Some organizations declare that they will review email messages regularly, and others state that email messages are private. In some states, if a company does not have a formal email policy, it can read email messages without employee notification.

Content Filtering

One of the more controversial issues that surround the Internet is its widespread availability of objectionable material, such as prejudiced literature, violence, and obscene photos. 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. Many businesses use content filtering to limit employees' web access. These businesses argue that employees are unproductive when visiting inappropriate or objectionable websites. Some schools, libraries, and parents use content filtering to restrict access to minors. Content filtering opponents argue that banning any materials violates constitutional guarantees of free speech and personal rights. Read Ethics & Issues 5-4 to consider whether content filtering violates first amendment rights.

ETHICS & ISSUES 5-4

Does Content Filtering in a Public Library Violate First Amendment Rights?

Among the resources libraries offer are Internet-enabled computers. The use of content filtering software on library computers controls the type of information a patron can access. Free speech advocates argue that this violates the First Amendment because it restricts library patrons from viewing certain websites and content.

The Children's Internet Protection Act (CIPA) requires that schools and libraries use content filtering software in order to receive certain federal funds. The purpose of CIPA is to restrict access to objectionable material, protect children when communicating online, prohibit children from sharing personal information, and restrict children's identities or accounts being hacked. Proponents of CIPA claim it is necessary to protect children. CIPA does allow libraries to turn off the filters, if an adult patrons requests it. Some libraries use content filtering software on computers used only by children.

Critics of content filtering software argue that the programs do not always work as intended. They can overfilter content, blocking information or education websites based on a single word. Some websites and services that filtering software may block include online social networks, or software platforms, such as Google Drive, which students may need to access to submit assignments. Conversely, they can underfilter content, which could result in access to webpages with inappropriate media. Others argue that it gives unequal access to students doing research who rely on library computers to do schoolwork and those who have unfiltered Internet access at home.

Libraries typically have a policy stating acceptable use of the Internet. Libraries' policies also should state whether they use content filtering software, so that the patrons are aware.

Consider This: Is it fair for a government to require that libraries use content filtering software? Why or why not? Do free speech laws cover content on the Internet? Why or why not?

Web filtering software is a program that restricts access to specified websites. Some also filter sites that use specific words (Figure 5-26). Others allow you to filter email messages, chat rooms, and programs. Many Internet security programs include a firewall, antivirus program, and filtering capabilities combined. Browsers also often include content filtering capabilities.

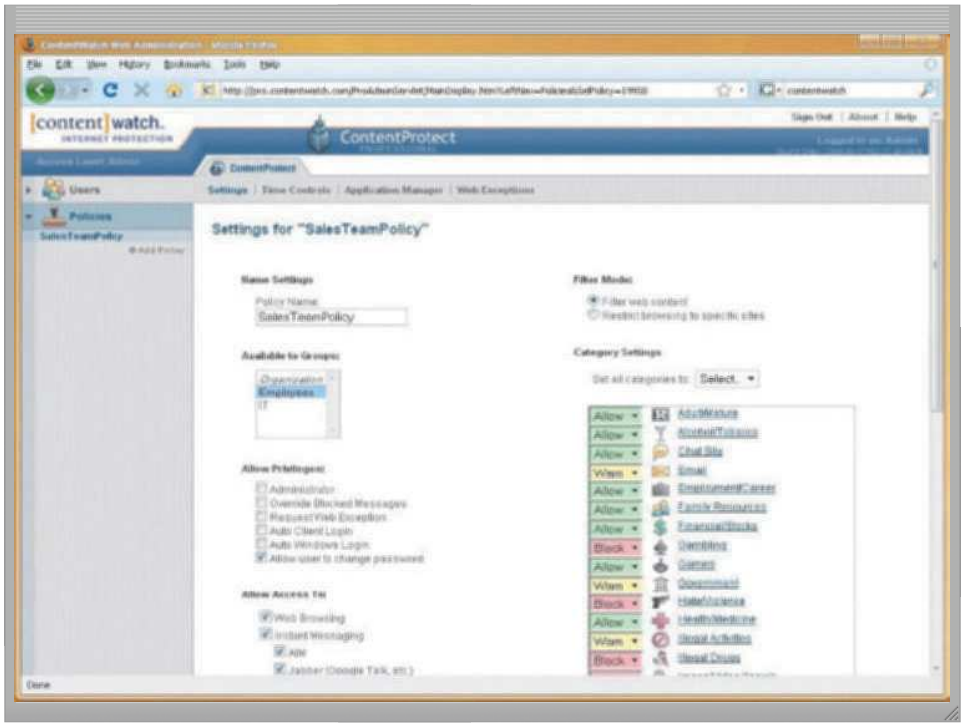


Figure 5-26 Web filtering software restricts access to specified websites.
Courtesy of ContentWatch, Inc.

NOW YOU SHOULD KNOW

Be sure you understand the material presented in the sections titled Ethics and Society and Information Privacy as it relates to the chapter objectives.
Now you should know …

- What issues you might encounter with respect to information accuracy, intellectual property, codes of conduct, and green computing (Objective 9)
- How you can make your personal data more private (Objective 10)
- Why your computer might have a cookie (Objective 10)

Discover More: Visit this chapter's premium content for practice quiz opportunities.

Chapter Summary

This chapter presented a variety of digital security risks. You learned about cybercrime and cybercriminals. The chapter discussed risks and safeguards associated with Internet and network attacks, unauthorized access and use, software theft, information theft, and hardware theft, vandalism, and failure. It presented various backup strategies and methods of securing wireless communications. You learned about ethical issues in society and various ways to protect the privacy of personal information.

Discover More: Visit this chapter's free resources for additional content that accompanies this chapter and also includes these features: Technology Innovators: AVG, Intel Security, Symantec, and LoJack; Technology Trends: Uses of Face Recognition Technology and Cloud Security; and High-Tech Talks: Digital Forensics and Encryption Algorithms.

Test your knowledge of chapter material by accessing the Study Guide, Flash Cards, and Practice Test resources from your smartphone, tablet, laptop, or desktop.

TECHNOLOGY @ WORK

National and Local Security

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, technology now assists 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 volume of criminal activity. For example, some cities are installing cameras in problematic areas. A 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 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 with 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 names on the No Fly List. If the computer finds a match, the individual must prove that he or she is not the person on the list before being allowed to board an aircraft.

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

Consider This: In what other ways do computers and technology play a role in national and local security?

© Dariusz Markowski / Photos.com

STUDENT ASSIGNMENTS

Study Guide

The Study Guide exercise reinforces material you should know for the chapter exam.

Discover More: Visit this chapter's premium content to **test your knowledge of digital content** associated with this chapter and **access the Study Guide resource** from your smartphone, tablet, laptop, or desktop.

Instructions: Answer the questions below using the format that helps you remember best or that is required by your instructor. Possible formats may include one or more of these options: write the answers; create a document that contains the answers; record answers as audio or video using a webcam, smartphone, or portable media player; post answers on a blog, wiki, or website; or highlight answers in the book/e-book.

1. Define the terms, digital security risk, computer crime, cybercrime, and crimeware.
2. Differentiate among hackers, crackers, script kiddies, cyberextortionists, and cyberterrorists. Identify issues with punishing cybercriminals.
3. List common types of malware. A(n) ___ is the destructive event or prank malware delivers.
4. Identify risks and safety measures when gaming.
5. Define these terms: botnet, zombie, and bot.
6. Describe the damages caused by and possible motivations behind DoS and DDoS attacks.
7. A(n) ___ allows users to bypass security controls when accessing a program, computer, or network.
8. Define the term, spoofing. How can you tell if an email is spoofed?
9. List ways to protect against Internet and network attacks.
10. Describe the purpose of an online security service.
11. Define the terms, firewall and proxy server. List steps to set up a personal firewall.
12. Give examples of unauthorized access and use of a computer or network.
13. Identify what an AUP should specify. Why might you disable file and printer sharing?
14. Explain how an organization uses access controls and audit trails.
15. Differentiate among user names, passwords, passphrases, and pass codes.
16. List tips for using a password manager safely.
17. What is a single sign on account? PIN stands for ___.
18. Describe the purpose of a CAPTCHA.
19. Define the terms, possessed objects and biometric devices.
20. What is the purpose of a lock screen?
21. Describe how companies use the following recognition, verification, or payment systems: fingerprint, face, hand, voice, signature, and iris. List disadvantages of biometric devices.
22. Explain the two-step verification process.
23. Define the term, digital forensics. Name areas in which digital forensics are used.
24. Define the terms, software theft, keygen, and software piracy. Identify methods to prevent software theft.
25. Explain the process of product activation.
26. Describe the following license agreement types: single- or end-user, network, and site. List conditions provided in a license agreement.
27. Give examples of information theft. How can you protect yourself from information theft?
28. Describe the functions of an encryption algorithm and an encryption key. Differentiate between private and public key encryption.
29. Unencrypted data is called ___; encrypted data is called ___.
30. Describe the purpose of a VPN.
31. Define these terms: digital signature, digital certificate, and secure site.
32. List concerns and responsibilities regarding cloud data storage and privacy.
33. Describe what occurs during hardware theft or vandalism.
34. Define the terms, backup and restore.
35. List six types of backups. Describe the three-generation backup policy.
36. Identify the components of a disaster recovery plan.
37. Describe security risks associated with wireless access. Identify ways to secure your wireless network.
38. List guidelines to protect your mobile device data.
39. Describe technology ethics, information accuracy, intellectual property rights, copyrights, and codes of conduct.
40. Describe issues surrounding inaccurate data.
41. List measures users can take to contribute to green computing.
42. Explain how companies, websites, and employers might infringe on your right to information privacy.
43. Describe how the following techniques are used to collect personal data: electronic profiles, cookies, phishing, clickjacking, spyware, adware, and madware.
44. How can you protect against phishing scams?
45. Identify methods to protect yourself from social engineering scams.
46. List examples of privacy laws. Should you be able to remove personal information from the Internet? Why or why not?
47. Describe what a company might track when monitoring employees.
48. Define and identify issues surrounding content and web filtering.
49. Describe uses of technology in the national and local security industry.

STUDENT ASSIGNMENTS

Key Terms

You should be able to define the Primary Terms and be familiar with the Secondary Terms listed below.

Discover More: Visit this chapter's premium content to **view definitions** for each term and to access the Flash Cards **resource** from your smartphone, tablet, laptop, or desktop.

Primary Terms

(shown in **bold-black** characters in the chapter)

adware (244)
back door (217)
back up (233)
backup (233)
biometric device (224)
botnet (216)
code of conduct (241)
computer crime (212)
content filtering (247)
cookie (243)
cracker (214)
cybercrime (212)
cyberextortionist (214)
cyberterrorist (214)
decrypt (229)
denial of service attack (DoS attack) (217)
digital certificate (231)
digital forensics (227)
digital security risk (212)
digital signature (231)
disaster recovery plan (234)
employee monitoring (247)
encryption (229)
fingerprint reader (224)
firewall (219)
green computing (241)
hacker (214)
information privacy (242)
information theft (229)
license agreement (228)
malware (215)
online security service (219)
password (222)
personal firewall (220)
phishing (244)
PIN (223)
piracy (228)
product activation (228)
restore (233)
script kiddie (214)
secure site (231)
social engineering (245)
software piracy (228)
software theft (228)
spoofing (217)
spyware (215)
technology ethics (238)
two-step verification (226)
user name (242)
web filtering software (248)
zombie (216)

Secondary Terms

(shown in *italic* characters in the chapter)

acceptable use policy (AUP) (231)
access control (222)
adware (215)
asymmetric key encryption (230)
audit trail (222)
biometric payment (226)
bot (216)
Business Software Alliance (BSA) (228)
CAPTCHA (224)
CERT/CC (219)
certificate authority (CA) (231)
child (234)
ciphertext (230)
clickjacking (245)
cloud backup (234)
Computer Emergency Response Team Coordination Center (219)
continuous data protection (CDP) (234)
copyright (240)
crimeware (212)
cyberforensics (227)
cyberwarfare (214)
cypher (230)
differential backup (234)
digital rights management (240)
distributed DoS attack (DDoS attack) (217)
email spoofing (217)
encryption algorithm (230)
encryption key (230)
end-user license agreement (EULA) (228)
ENERGY STAR program (241)
face recognition system (225)
full backup (234)
grandparent (234)
hacktivist (214)
hand geometry system (225)
incremental backup (234)
intellectual property (IP) (240)
intellectual property rights (240)
IP spoofing (217)
keygen (228)
lock screen (225)
MAC address (236)
MAC address control (236)
madware (245)
malicious software (215)
network license (229)
off-site (233)
parent (234)
passcode (223)
passphrase (223)
password manager (223)
password organizer (223)
payload (215)
phishing filter (244)
plaintext (230)
power usage effectiveness (PUE) (241)
private key encryption (230)
proxy server (219)
public key encryption (230)
rootkit (215)
selective backup (234)
session cookie (243)
signature verification system (225)
single sign on (222)
single-user license agreement (228)
site license (229)
spyware (215)
SSID (236)
symmetric key encryption (230)
trojan horse (215)
two-factor verification (226)
unauthorized access (221)
unauthorized use (221)
user ID (222)
virtual private network (VPN) (230)
virus (215)
voice verification system (225)
worm (215)
zombie army (216)

Carnegie Mellon University

CAPTCHA (224)

STUDENT ASSIGNMENTS

Checkpoint

The Checkpoint exercises test your knowledge of the chapter concepts. The page number containing the answer appears in parentheses after each exercise. The Consider This exercises challenge your understanding of chapter concepts.

Discover More: Visit this chapter's premium content to **complete the Checkpoint exercises interactively;** complete the **self-assessment in the Test Prep resource** from on your smartphone, tablet, laptop, or desktop; and then **take the Practice Test.**

True/False

Mark T for True and F for False.

_____ 1. Any illegal act involving the use of a computer or related devices generally is referred to as a crimeware. (212)

_____ 2. A rootkit displays an online advertisement in a banner or pop-up window on webpages, email, or other Internet services. (215)

_____ 3. Viruses, worms, and other malware can be hidden in downloaded game files and mobile apps. (216)

_____ 4. An audit trail records in a file both successful and unsuccessful access attempts. (222)

_____ 5. It is good practice to change your password frequently. (222)

_____ 6. Intentionally erasing software would be considered software theft. (228)

_____ 7. A typical license agreement allows you to rent or lease the software. (229)

_____ 8. Unencrypted, readable data is called ciphertext. (230)

_____ 9. Private key encryption also is called asymmetric key encryption. (230)

_____ 10. VPNs encrypt data to help ensure that the data is safe from being intercepted by unauthorized people. (230)

_____ 11. When data is traveling to or from a computer to a cloud service, it is subject to interception. (232)

_____ 12. A good practice to secure your wireless network is to immediately broadcast the SSID. (236)

Multiple Choice

Select the best answer.

1. A _____ is someone who demands payment to stop an attack on an organization's technology infrastructure. (214)
   a. cyberterrorist
   b. script kiddie
   c. cracker
   d. cyberextortionist

2. _____ is a program that hides in a computer or mobile device and allows someone from a remote location to take full control of the computer or device. (215)
   a. A rootkit
   b. Spyware
   c. A trojan horse
   d. Adware

3. A ____ is a program or set of instructions in a program that allows users to bypass security controls when accessing a program, computer, or network. (217)
   a. zombie
   b. botnet
   c. back door
   d. session cookie

4. An employee using an organization's computer to send personal email messages might be an example of _____. (221)
   a. cybercrime
   b. hardware vandalism
   c. intellectual property rights violation
   d. unauthorized access and use

5. A _____ is a private combination of words, often up to 100 characters in length and containing mixed capitalization and punctuation, associated with a user name that allows access to certain computer resources. (223)
   a. passphrase
   b. private key
   c. passcode
   d. encryption algorithm

6. A(n) _____ is a set of characters that the originator of the data uses to encrypt the text and the recipient of the data uses to decrypt the text. (230)
   a. cipher
   b. plaintext
   c. public key
   d. encryption key

7. A(n) _____ backup method is the only real-time back up, providing very fast recovery of data. (234)
   a. selective
   b. full
   c. incremental
   d. continuous data protection

8. Online shopping websites generally use a _____ to keep track of items in a user's shopping cart. (243)
   a. phishing filter
   b. session cookie
   c. location sharing algorithm
   d. keygen

Checkpoint

STUDENT ASSIGNMENTS

Matching Match the terms with their definitions.

_____ 1. script kiddie (214)
_____ 2. zombie (216)
_____ 3. bot (216)
_____ 4. spoofing (217)
_____ 5. access control (222)
_____ 6. keygen (228)
_____ 7. digital certificate (231)
_____ 8. technology ethics (238)
_____ 9. digital rights management (240)
_____ 10. cookie (243)

a. compromised computer or device whose owner is unaware the computer or device is being controlled remotely by an outsider
b. technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network
c. program that performs a repetitive task on a network
d. small text file that a web server stores on your computer
e. notice that guarantees a user or website is legitimate
f. strategy designed to prevent illegal distribution of movies, music, and other digital content
g. program that creates software registration numbers and sometimes activation codes
h. hacker who does not have the technical skills and knowledge of a cracker
i. security measure that defines who can access a computer, device, or network; when they can access it; and what actions they can take while accessing it
j. moral guidelines that govern the use of computers, mobile devices, information systems, and related technologies

Consider This Answer the following questions in the format specified by your instructor.

1. Answer the critical thinking questions posed at the end of these elements in this chapter: Ethics & Issues (214, 233, 246, 247), How To (218, 221, 236, 244), Mini Features (232, 235, 237), Secure IT (216, 219, 223, 240), and Technology @ Work (249).
2. What are some common digital security risks? (212)
3. How does a hacker differ from a cracker? (214)
4. What is cyberwarfare? (214)
5. What is a hacktivist? (214)
6. How does malware deliver its payload? (215)
7. What is a botnet? (216)
8. What practices should gamers follow to increase their security? (216)
9. What is the purpose of a DoS attack? (217)
10. Why would a programmer or computer repair technician build a back door? (217)
11. How is email spoofing commonly used? (217)
12. What are methods to protect computers, mobile devices, and networks from attacks? (218)
13. Who would an organization requiring assistance or information about Internet security breach contact? (219)
14. What screening techniques do proxy servers use? (219)
15. How does unauthorized access differ from unauthorized use? (221)
16. What is a single sign-on account? (222)
17. What is a password manager? (223)
18. Are passphrases more secure than passwords? Why or why not? (223)
19. How are fingerprint readers used with personal computers and mobile devices? (225)
20. What conditions are found in a typical single-user license agreement? (229)
21. Who issues digital certificates? (231)
22. What is meant by a three-generation backup policy? (234)
23. What should you include in a disaster recovery plan for natural disasters? What should you include for man-made disasters? (235)
24. What steps can you take to secure your wireless network? (236)
25. How can mobile security apps protect your mobile device data? (237)
26. What are some questions that arise surrounding fair use with respect to copyrighted material? (240)
27. What role does the ENERGY STAR program play in green computing? (241)
28. For what purposes do websites use cookies? (243)
29. What is clickjacking? (245)

STUDENT ASSIGNMENTS

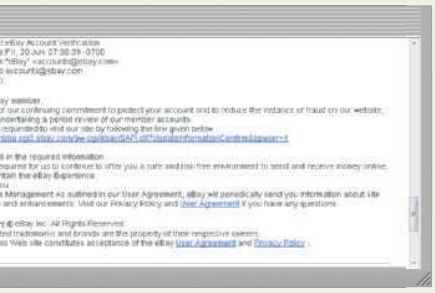
Problem Solving

The Problem Solving exercises extend your knowledge of chapter concepts by seeking solutions to practical problems with technology that you may encounter at home, school, work, or with nonprofit organizations. The Collaboration exercise should be completed with a team.

Instructions: You often can solve problems with technology in multiple ways. Determine a solution to the problems in these exercises by using one or more resources available to you (such as a computer or mobile device, articles on the web or in print, blogs, podcasts, videos, television, user guides, other individuals, electronics or computer stores, etc.). Describe your solution, along with the resource(s) used, in the format requested by your instructor (brief report, presentation, discussion, blog post, video, or other means).

Personal

1. **No Browsing History** While using the browser on your tablet, you realize that it is not keeping a history of websites you have visited. Why might this be happening, and what is the first step you will take to correct this problem?
2. **Phishing Scam** You just received an email message from someone requesting personal identification information.



Source: Privacy Rights Clearinghouse

Believing the message was legitimate, you provided the requested information to the original sender. You now realize, however, that you might have fallen victim to a phishing scam. What are your next steps?

3. **Suspicious File Attachment** You receive an email message that appears to be from someone you know. When you try to open the attachment, nothing happens. You attempt to open the attachment two more times without any success. Several minutes later, your computer is running slower and you are having trouble running apps. What might be wrong?
4. **Antivirus Software Outdated** After starting your computer and signing in to the operating system, a message is displayed stating that your virus definitions are out of date and need to be updated. What are your next steps?
5. **Laptop's Physical Security** You plan to start taking your laptop to school so that you can record notes in class. You want to make sure, however, that your computer is safe if you ever step away from it for a brief period of time. What steps can you take to ensure the physical security of your laptop?

Professional

6. **Corporate Firewall Interference** You installed a new browser on your work computer because you no longer wish to use the default browser provided with the operating system. When you run the new browser, an error message appears stating that a user name and password are required to configure the firewall and allow this program to access the Internet. Why has this happened?
7. **Problems with CAPTCHA** You are signing up for an account on a website and encounter a CAPTCHA. You attempt to type the characters you see on the screen, but an error message appears stating that you have entered the incorrect characters. You try two more times and get the same result. You are typing the characters to the best of your ability but think you still might be misreading at least one of the characters. What are your next steps?
8. **Unclear Acceptable Use Policy** You read your company's acceptable use policy, but it is not clear about whether you are able to use the computer in your office to visit news websites on your lunch break. How can you determine whether this type of activity is allowed?
9. **Two-Step Verification Problem** A website you are attempting to access requires two-step verification. In addition to entering your password, you also have to enter a code that it sends to you as a text message. You no longer have the same phone number, so you are unable to receive the text message. What are your next steps?
10. **Issue with Virus Protection** You receive a notification that the antivirus program on your computer is not enabled. While attempting to enable the antivirus program, an error message is displayed stating that a problem has prevented the antivirus program from being enabled. What are your next steps?

Collaboration

11. **Technology in National and Local Security** National and local security agencies often use technology to protect citizens. For example, computers are used to maintain a No Fly List, which contains 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 technology helps to keep the public safe. One team member should research how local agencies, such as police departments, use technology to ensure security. Another team member should research ways national security agencies use technology to protect the public from threats, and the last team member should research ways that private businesses use technology to enhance security. Compile these findings into a report and submit it to your instructor.

How To: Your Turn

The How To: Your Turn exercises present general guidelines for fundamental skills when using a computer or mobile device and then require that you determine how to apply these general guidelines to a specific program or situation.

Discover More: Visit this chapter's premium content to **challenge yourself with additional How To: Your Turn exercises,** which include App Adventure.

Instructions: You often can complete tasks using technology in multiple ways. Figure out how to perform the tasks described in these exercises by using one or more resources available to you (such as a computer or mobile device, articles on the web or in print, online or program help, user guides, blogs, podcasts, videos, other individuals, trial and error, etc.). Summarize your 'how to' steps, along with the resource(s) used, in the format requested by your instructor (brief report, presentation, discussion, blog post, video, or other means).

1 Evaluating Your Electronic Profile

When you make purchases online, tap or click advertisements, follow links, and complete online forms requesting information about yourself, you are adding to your electronic profile. While an electronic profile may help businesses guide you toward products and services that are of interest to you, some people view them as an invasion of privacy. The following steps guide you through the process of locating online information about yourself and taking steps to remove the information, if possible.

a. Run a browser.
b. Navigate to a search engine of your choice.
c. Perform a search for your full name.
d. In the search results, follow a link that you feel will display a webpage containing information about you. If the link's destination does not contain information about you, navigate back to the search results and follow another link.
e. Evaluate the webpage that contains information about you. If you wish to try removing the information, locate a link that allows you to contact the site owner(s) or automatically request removal of the information.
f. Request that your information be removed from the website. Some websites may not honor your request for removal. If you feel that the information must be removed, you may need to solicit legal advice.
g. If the search results display information from an account you have on an online social network, such as Facebook or LinkedIn, you may need to adjust your privacy settings so that the information is not public. If the privacy settings do not allow you to hide your information, you may need to consider deleting the account.
h. Repeat Steps d – g for the remaining search results. When you no longer see relevant search results for the search engine you used, search for other variations of your name (use your middle initial instead of your middle name, exclude your middle name, or consider using commonly used nicknames instead of your first name).
i. Use other search engines to search for different variations of your name. Some search engines uncover results that others do not.
j. If you have an account on an online social network, navigate to the website's home page and, without signing in, search for your name. If information appears that you do not want to be public, you may need to adjust your privacy settings or remove your account.
k. Follow up with requests you have made to remove your online information.

Exercises

1. What personal information have you uncovered online? Did you have any idea that the information was there?
2. What additional steps can you take to prevent people and businesses from storing information about you?
3. What steps might you be able to take if you are unsuccessful with your attempts to remove online information that identifies you?

Source: Geoffrey, LLC

STUDENT ASSIGNMENTS

How To: Your Turn

2 Update Virus Definitions

In addition to installing or activating an antivirus program on your computer or mobile device to keep it safe from viruses, it also is necessary to keep the virus definitions updated so that the antivirus program can search for and detect new viruses on your computer or mobile device. New virus definitions can be released as often as once per day, depending on the number of new viruses that are created. Antivirus programs either can search for and install new virus definitions automatically at specified intervals, or you can update the virus signatures manually. The following steps describe how to update the virus definitions for an antivirus program.

Update Virus Definitions Manually

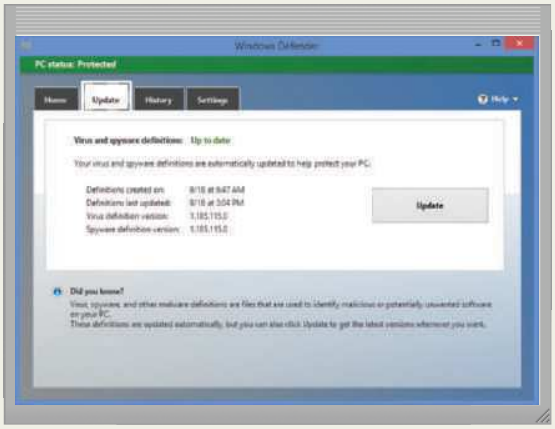
a. If necessary, establish an Internet connection so that you will be able to update the virus definitions.
b. Run an antivirus program.
c. Tap or click the button to check for updated virus definitions.
d. If new virus definitions are available for the antivirus program, tap or click the link to download the definitions to the computer or mobile device.
e. When the update is complete, tap or click the button to scan the computer or mobile device for viruses.

Configure Automatic Updates for Virus Definitions

a. If necessary, establish an Internet connection so that you will be able to update the virus definitions.
b. Run an antivirus program.
c. Tap or click the option to update virus definitions automatically.
d. Tap or click the option to display the virus definition update schedule.
e. To provide the maximum protection from viruses, configure the antivirus program to update definitions as frequently as possible.
f. After configuring the update schedule, tap or click the button to update virus definitions manually.
g. When the update is complete, tap or click the button to scan the computer or mobile device for viruses.

Exercises

1. What antivirus program, if any, currently is installed on your computer? Is it scheduled to update virus definitions automatically?
2. In addition to downloading and installing virus definitions from within the antivirus program, are other ways available to obtain the latest virus definitions?
3. In addition to keeping the antivirus program's virus definitions current, what other ways can you protect a computer or mobile device from viruses?



Source: Microsoft

3 Determine Whether a Computer or Mobile Device Is Secured Properly

Several steps are required to secure a computer or mobile device properly. In addition to installing antivirus software and updating the virus definitions regularly, you also should install and configure a firewall, keep the operating system up to date, and be careful not to open suspicious email messages, visit unsecure webpages, or download untrusted files while using the Internet. The following steps guide you through the process of making sure your computer or mobile device is secured properly by verifying antivirus software is installed and running, a firewall is enabled and configured, and the operating system is up to date.

Verify Antivirus Software

a. Use the search tool in the operating system or scan the programs on the computer or mobile device for antivirus software. Some operating systems include antivirus software.
b. If you are unable to locate antivirus software on the computer or mobile device, obtain an antivirus program and install it.
c. Run the antivirus program.
d. Verify the virus definitions in the antivirus program are up to date.

Verify the Firewall

a. Use the search tool in the operating system or scan the programs, apps, and settings on the computer or mobile device to access and configure the firewall.
b. If you are unable to locate a firewall on the computer or mobile device, obtain a firewall program and install it.
c. Run the firewall program.
d. View the firewall settings and verify the firewall is turned on.
e. View the list of programs, apps, and features allowed through the firewall. If you do not recognize or use one or more of the programs, apps, or features, remove them from the list of allowed programs, apps, and features.

Verify Operating System Updates

a. If necessary, establish an Internet connection.
b. Navigate to the area of the operating system where you can access the button, link, or command to search for operating system updates. For example, in Microsoft Windows, you would display the settings for Windows Update.
c. Tap or click the button, link, or command to check for updates.
d. If no updates are available, your operating system is up to date. If the operating system locates additional updates, download and install the updates. **NOTE: If the computer or mobile device you are using does not belong to you, check with its owner before downloading and installing updates for the operating system.**

Source: Microsoft

Exercises

1. Before you began this exercise, was your computer or mobile device secured properly? How did you know your computer or mobile device was secured properly? If it was not, what actions did you need to perform to secure it?
2. Which programs, apps, and features do you think are safe to allow through your firewall? Which programs, apps, and features do you feel are not safe to allow through your firewall?
3. What additional ways can you properly secure your computer?

4 Clear Your Browsing History

A browser keeps track of the webpages that you have visited previously unless you have changed your settings. Although you can clear the browsing history on your computer or mobile device, your Internet service provider still may have logs that show a history of websites you have visited. The following steps guide you through the process of clearing your browsing history.

a. Run the browser.
b. Display the browser's settings.
c. If necessary, navigate to the settings that configure the browser's security settings. These settings often are found in the Security, Safety, or Privacy category.
d. Select the option to delete the browsing history. In addition to deleting the list of websites you have visited, you also may be able to clear passwords the browser has remembered, clear cookies and temporary internet files, clear data you entered in forms, and clear a history of downloads.
e. When the browsing history has been deleted, run the browser again.
f. Follow the above steps for each additional browser you have installed on your computer or mobile device.

Exercises

1. What are some reasons why you might want to delete your browsing history?
2. Can you configure your browser to automatically delete your browsing history? If so, how?
3. What are the advantages of keeping your browsing history? If you do keep your browsing history, how long do you keep it?

5 Configure a Browser's Cookie Settings

As discussed in this chapter, cookies can be used for a variety of reasons. Websites can install cookies on your computer or mobile device that can store information on your computer or mobile device, or track your browsing habits. You can configure a browser's settings to disallow websites from storing and accessing cookies on your computer or mobile device. The following steps guide you through the process of configuring a browser's cookie settings.

a. Run the browser.
b. Display the browser's settings.
c. Navigate to the settings that configure the browser's cookie settings. These settings often are found in the Security, Safety, or Privacy category.
d. Configure how the browser handles first-party cookies and third-party cookies. Some users choose to reject all cookies. To function properly, however, some websites require that you accept their cookies.
e. Save the changes to the settings.
f. Run the browser again.

Exercises

1. What is the difference between first-party cookies and third-party cookies?
2. Configure the browser to deny all first-party and third-party cookies and then navigate to five websites you visit most frequently. Do the websites display any differently now that you are denying all cookies? Describe your browsing experience while the browser is configured to deny all cookies.
3. What security risks are associated with cookies?

STUDENT ASSIGNMENTS

Internet Research

The Internet Research exercises broaden your understanding of chapter concepts by requiring that you search for information on the web.

Discover More: Visit this chapter's premium content to **challenge yourself with additional Internet Research exercises,** which include Search Sleuth, Green Computing, Ethics in Action, You Review It, and Exploring Technology Careers.

Instructions: Use a search engine or another search tool to locate the information requested or answers to questions presented in the exercises. Describe your findings, along with the search term(s) you used and your web source(s), in the format requested by your instructor (brief report, presentation, discussion, blog post, video, or other means).

1 Making Use of the Web

News, Weather, and Sports

Apps on tablets, smartphones, and other mobile devices are changing the delivery of the day's major news, weather, and sports stories. In one study, approximately one-half of American adults reported that they get some of their news on a tablet or mobile device. They view video and photos from eyewitnesses and fans, read analyses from investigators and coaches, and comment on stories. Men and college-educated people are the heaviest users of mobile news websites, and they are likely to read in-depth investigations and analyses. Online social networks also are a major source of information for many people.

Research This: (a) Visit two news websites or apps and locate one national event covered in both sources. Compare the coverage of the two stories. What information is provided in addition to the text, such as video, graphics, or links to related articles? Which story offers a better analysis? Which source is easier to navigate and read? Then, using another website or app, locate and read today's top international news story. What did you learn by reading the story? Were you aware of this event prior to reading the online story? Does the coverage include videos and photos to increase your comprehension?

(b) Visit a weather website or app and obtain the five-day forecast for your hometown. Include details about information that supplements the current and forecast conditions, such as a pollen or air quality index, storm tracking, travel advisories, or season summaries.

Source: National Weather Service

(c) Visit a sports website or app and read the first story reported. Describe the coverage of this event. Which sources are quoted in the story? Which links are included to other stories? Describe the features provided on this website, such as the ability to chat, customize the page for your favorite teams, or share the content with media sharing sites.

2 Social Media

Sharing photos on your social media sites of yesterday's visit to the ballpark might be at the top of today's to-do list, but these images might be just the clues cyberthieves need to access your account. Facebook, in particular, is one website that scammers and advertisers use to gather information regarding your whereabouts and your personal life. Their malicious attacks begin with a visit to your timeline or other record of your activities. Searching for keywords on your page, they send targeted messages appearing to originate from trusted friends. If you open their attachments or tap or click their links, you have given these unscrupulous individuals access to your account. In addition, you may think you have crafted a password no one could guess. With your page open for others to view, however, the thieves scour the contents in hopes of locating starting clues, such as children's names, anniversary dates, and pet breeds, which could be hints to cracking your password.

Research This: In the Help section of an online social network you use, search for information about changing your profile's security and privacy settings. What steps can you take to mitigate the chance of becoming the victim of a hack? For example, can you adjust the connection settings to restrict who can see stories, send friend requests and messages, or search for you by name or contact information? Can you hide certain posts or block people from posting on your page? Can you report posts if they violate the website's terms? What are other potential threats to someone accessing your account?

3 Search Skills

Social Media Search

Search engines provide access to millions of search results by finding webpages, documents, images, or

Internet Research

other information that match the search text you provide. Recommendations from people who use social media to share what they have read can be a possible alternative to using a search engine. People who take the time to Tweet pin an article or image on Twitter or Pinterest often do so because they found it useful, and hope others will as well.

To search Twitter, type the search text, search twitter, in a search engine to find the web address for the Twitter Search website, or sign in to Twitter with your credentials. In the Search Twitter text box, type the search text. For example, type the text, best mapping app, to find recommendations of links to articles or websites about mapping apps. You also can search Twitter for hashtags (a keyword preceded by a # symbol) to find Tweets about current events or popular discussion topics.

To search Pinterest, sign in to your Pinterest account and then type the search text into the search box. For example, type the search text, information security, into the search box to view related pins from Pinterest users. Pinterest users often pin links to infographics, images, and websites.

Source: Pinterest

Research This: Use Twitter and Pinterest to search for information about the following topics and then compare your results with those you would find using a search engine such as Bing, Google, or Yahoo!. (1) green computing, (2) computer virus, (3) cybercrime, and (4) malware. How are the results different? What type of information are you more likely to find on Twitter, on Pinterest, and using a search engine?

4 Security

Digital certificates and signatures detect a sender's identity and verify a document's authenticity. In this chapter you learned that many e-commerce companies use them in an attempt to prevent digital eavesdroppers from intercepting confidential information. The online certificate authority (CA) vendors generate these certificates using a standard, called X.509, which is coordinated by the International Telecommunication Union and uses algorithms and encryption technology to identify the documents.

Research This: Visit websites of at least two companies that issue digital certificates. Compare products offered, prices, and certificate features. What length of time is needed to issue a certificate? What is a green address bar, and when is one issued? What business or organization validation is required? Then, visit websites of at least two companies that provide digital signatures. Compare signing and sending requirements, types of supported signatures, and available security features. Which documents are required to obtain a digital signature? When would a business need a Class 2 rather than a Class 3 digital signature?

5 Cloud Services

Cloud Security (SecaaS)

Antivirus software offers regular, automatic updates in order to protect a server, computer, or device from viruses, malware, or other attacks. Antivirus software is an example of cloud security, or security as a service (SecaaS), a service of cloud computing that delivers virus definitions and security software to users over the Internet as updates become available, with no intervention from users. Security as a service is a special case of software as a service, but is limited to security software solutions.

Individuals and enterprise users take advantage of antivirus software and security updates. Enterprise cloud users interact with cloud security solutions via a web interface to configure apps that provide protection to email servers, preventing spam before it arrives, keeping data secure, and watching for online threats and viruses. As the use of cloud-based resources continues, the market for security as a service solutions is expected to increase significantly in coming years.

Research This: (1) Use a search engine to find two different providers of security as a service solutions. Research the different solutions they provide, and report your findings. (2) How are enterprise security requirements different from those of individual users?

STUDENT ASSIGNMENTS

Critical Thinking

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

Instructions: Evaluate the situations below, using personal experiences and one or more resources available to you (such as articles on the web or in print, blogs, podcasts, videos, television, user guides, other individuals, electronics or computer stores, etc.). Perform the tasks requested in each exercise and share your deliverables in the format requested by your instructor (brief report, presentation, discussion, blog post, video, or other means).

1. Online Gaming Safety

You and your friend frequently play a popular online role-playing game. Your friend's computer had a virus recently, which was traced back to a malware-infected website. Your friend tells you that she visited the website after following a link while playing the game. What risks are involved when playing online games?

Do This: Use the web to find articles about incidents of malware infections associated with online gaming. Research tips for increasing security when playing online games. Did you find other threats and security tips in addition to the ones mentioned in this chapter? Have you ever downloaded updates to a game? If so, how did you ensure the updates were safe? Locate a list of games that are known to cause malware infections. Share your findings and any online gaming security problems you have experienced with the class.

2. Ensuring Safety and Security Online

You work in the information technology department for a large enterprise. An increasing number of users are contacting the help desk complaining about slow computer performance. Help desk representatives frequently attribute the decreased performance to malware. Although the help desk has installed security software on each computer, users also must practice safe computing. Your manager asked you to prepare information that teaches employees how to guard against malware and other security threats.

Do This: Include information such as how to determine if a website is safe, how to identify email and other spoofing schemes, guidelines for downloading programs and apps, email attachment safety, and how to avoid phishing scams. Create a list of how organizations use common safeguards to protect other users on the network, such as firewalls, proxy servers, user names and passwords, access controls, and audit trails.

3. Case Study

Amateur Sports League You are the new manager for a nonprofit amateur soccer league. The league's board of directors asked you to develop a disaster recovery plan for its main office. The main office consists of a small storefront with two back rooms: one room is the office, with all of the electronic equipment and paper files; the other is for storage of nonelectronic equipment. The staff members — you, an administrative assistant, and an information technology (IT) specialist — work in the office. The electronic equipment in the office includes two desktops, a laptop, an external hard drive for backups, a wireless router, and two printers. In addition, each staff member has a smartphone.

Do This: Choose either a natural or man-made disaster. Create a disaster recovery plan that outlines emergency strategies, backup procedures, recovery steps, and a test plan. Assign staff members roles for each phase of the disaster recovery plan.

Collaboration

4. Implementing Biometric Security

You are the chief technology officer of a large company. You have been reading an article about computer security that discussed several examples of security breaches, including thieves breaking into an office and stealing expensive equipment, and a recently terminated employee gaining access to the office after hours and corrupting data. Because of these incidents, your company would like to start using biometric devices to increase its security.

Do This: Form a three-member team and research the use of biometric devices to protect equipment and data. Each member of your team should choose a different type of biometric device, such as fingerprint readers, face recognition systems, and hand geometry systems. Find products for each device type, and research costs and user reviews. Search for articles by industry experts. Would you recommend using the biometric device for security purposes? Why or why not? Meet with your team, discuss and compile your findings, and then share with the class.

Courtesy of Ingersoll Rand Security Technologies

Technology Timeline

1937 Dr. John V. Atanasoff and Clifford Berry design and build the first electronic digital computer. Their machine, the Atanasoff-Berry-Computer, or ABC, provides the foundation for advances in electronic digital computers.

AP Images/Frederick News-Post (2); J. R. Eyerman/The LIFE Picture Collection/Getty Images

1945 John von Neumann poses in front of the electronic computer built at the Institute for Advanced Study. This computer and its von Neumann architecture served as the prototype for subsequent stored program computers worldwide.

Photo: Alan Richards, from the Shelby White and Leon Levy Archives Center, Institute for Advanced Study, Princeton, NJ, USA (2)

1947 William Shockley, John Bardeen, and Walter Brattain invent the transfer resistance device, eventually called the transistor. The transistor would revolutionize computers, proving much more reliable than vacuum tubes.

© IBM Corporate Archives (2)

1952 Dr. Grace Hopper considers the concept of reusable software in her paper, "The Education of a Computer." The paper describes how to program a computer with symbolic notation instead of detailed machine language.

Courtesy of Hagley Museum and Library

1937 | 1943 | 1945 | 1946 | 1947 | 1951 | 1952 | 1953

Bletchley Park Trust/SSPL/The Image Works

S.M./Sueddeutsche Zeitung Photo/The Image Works

1943 During World War II, British scientist Alan Turing designs the Colossus, an electronic computer created for the military to break German codes. The computer's existence is kept secret until the 1970s.

Source: U.S. Army

1946 Dr. John W. Mauchly and J. Presper Eckert, Jr. complete work on the first large-scale electronic, general-purpose digital computer. The ENIAC (Electronic Numerical Integrator And Computer) weighs 30 tons, contains 18,000 vacuum tubes, occupies a 30 × 50 foot space, and consumes 160 kilowatts of power.

Courtesy Unisys Corporation

1951 The first commercially available electronic digital computer, the UNIVAC I (UNIVersal Automatic Computer), is introduced by Remington Rand. Public awareness of computers increases when the UNIVAC I correctly predicts that Dwight D. Eisenhower will win the presidential election.

© IBM Corporate Archives

1953 Core memory, developed in the early 1950s, provides much larger storage capacity than vacuum tube memory.

1953 The IBM model 650 is one of the first widely used computers. The computer is so successful that IBM manufactures more than 1,000. IBM will dominate the mainframe market for the next decade.

1957 The IBM 305 RAMAC computer is the first to use magnetic disk for external storage. The computer provides storage capacity similar to magnetic tape that previously was used but offers the advantage of semi-random access capability.

© IBM Corporate Archives

© IBM Corporate Archives

1957 FORTRAN (FORmula TRANslation), an efficient, easy-to-use programming language, is introduced by John Backus.

1959 More than 200 programming languages have been created.

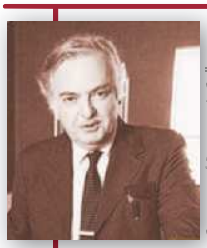
1959 IBM introduces two smaller, desk-sized computers: the IBM 1401 for business and the IBM 1620 for scientists.

© IBM Corporate Archives

1965 Digital Equipment Corporation (DEC) introduces the first microcomputer, the PDP-8. The machine is used extensively as an interface for time-sharing systems.

Courtesy of Hewlett-Packard Company

1965 Dr. John Kemeny of Dartmouth leads the development of the BASIC programming language.



Courtesy of Dartmouth College

1968 In a letter to the editor titled, "GO TO Statements Considered Harmful," Dr. Edsger Dijkstra introduces the concept of structured programming, developing standards for constructing computer programs.

1968 Computer Science Corporation (CSC) becomes the first software company listed on the New York Stock Exchange.

© Cengage Learning

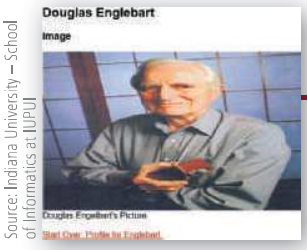
1957 | 1958 | 1959 | 1960 | 1964 | 1965 | 1967 | 1968

Courtesy of Texas Instruments (2)

1958 Jack Kilby of Texas Instruments invents the integrated circuit, which lays the foundation for high-speed computers and large-capacity memory. Computers built with transistors mark the beginning of the second generation of computer hardware.

Courtesy of Hagley Museum and Library

1960 COBOL, a high-level business application language, is developed by a committee headed by Dr. Grace Hopper.



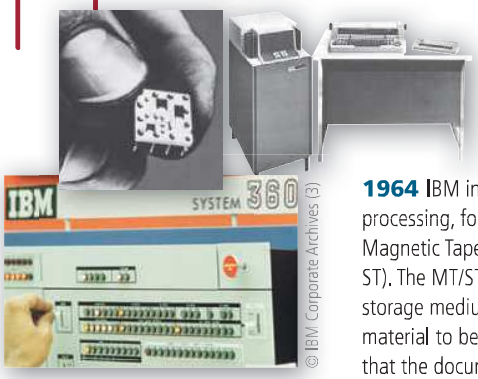
Source: Indiana University – School of Informatics at IUPUI

1967 Douglas Engelbart applies for a patent for his wooden mouse.

1964 The number of computers has grown to 18,000. Third-generation computers, with their controlling circuitry stored on chips, are introduced. The IBM System/360 computer is the first family of compatible machines, merging science and business lines.

© IBM Corporate Archives

1968 Alan Shugart at IBM demonstrates the first regular use of an 8-inch floppy disk.



© IBM Corporate Archives (3)

1964 IBM introduces the term, word processing, for the first time with its Magnetic Tape/Selectric Typewriter (MT/ST). The MT/ST was the first reusable storage medium that allowed typed material to be edited without requiring that the document be retyped.

1969 Under pressure from the industry, IBM announces that some of its software will be priced separately from the computer hardware, allowing software firms to emerge in the industry.

© IBM Corporate Archives

1969 The ARPANET network is established, which eventually grows to become the Internet.

1975 MITS, Inc. advertises one of the first microcomputers, the Altair. The Altair is sold in kits for less than $400, and within the first three months 4,000 orders are taken.

LiPo Ching/MCT/Newscom

1975 Ethernet, the first local area network (LAN), is developed at Xerox PARC (Palo Alto Research Center) by Robert Metcalfe.

1976 Steve Jobs and Steve Wozniak build the first Apple computer. A subsequent version, the Apple II, is an immediate success. Adopted by elementary schools, high schools, and colleges, for many students, the Apple II is their first contact with the world of computers.

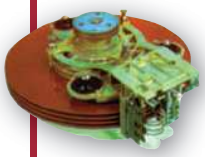
LongHa2006/iStockphoto.com

© Bettmann/CORBIS

1980 IBM offers Microsoft Corporation cofounder, Bill Gates, the opportunity to develop the operating system for the soon-to-be announced IBM personal computer. With the development of MS-DOS, Microsoft achieves tremendous growth and success.

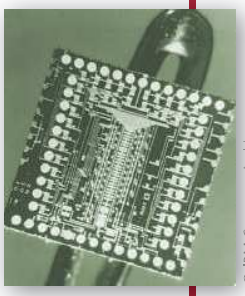
Courtesy of IBM Corporate Archives

1980 Alan Shugart presents the Winchester hard disk, revolutionizing storage for personal computers.



Courtesy of IBM Corporate Archives

1969 | 1970 | 1971 | 1975 | 1976 | 1979 | 1980 | 1981



© IBM Corporate Archives

1970 Fourth-generation computers, built with chips that use LSI (large-scale integration) arrive. While the chips used in 1965 contained up to 1,000 circuits, the LSI chip contains as many as 15,000.

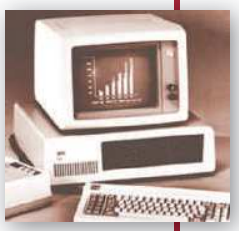
Courtesy of Intel Corporation (2)

1971 Dr. Ted Hoff of Intel Corporation develops a microprocessor, or microprogrammable computer chip, the Intel 4004.

1979 VisiCalc, a spreadsheet program written by Bob Frankston and Dan Bricklin, is introduced.

1979 The first public online information services, CompuServe and the Source, are founded.

1981 The IBM PC is introduced, signaling IBM's entrance into the personal computer marketplace. The IBM PC quickly garners the largest share of the personal computer market and becomes the personal computer of choice in business.



Courtesy of IBM Corporate Archives

1981 The first computer virus, Elk Cloner, is spread via Apple II floppy disks, which contained the operating system. A short rhyme would appear on the screen when the user pressed the Reset button after the 50th boot of an infected disk.

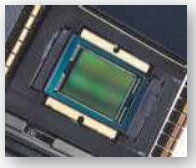
© Rebecca Lowe/iStockphoto


© Lane V. Erickson/Shutterstock
Courtesy of Microsoft® Corporation

1986 Microsoft has public stock offering and raises approximately $61 million.

1988 Microsoft surpasses Lotus Development Corporation to become the world's top software vendor.

1991 Kodak announces the first digital SLR (single-lens reflex) camera. The Kodak DCS 100 is developed mostly for photojournalism purposes and stores the photos and batteries in a separate unit.


©NMPFT/SSPL / The Image Works

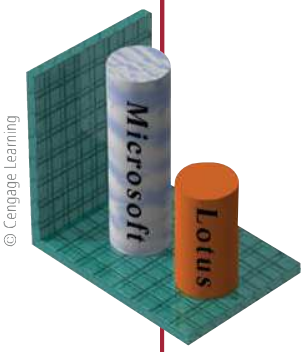

3.275 Million

1982 3,275,000 personal computers are sold, almost 3,000,000 more than in 1981.

1982 Hayes introduces the 300 bps smart modem. The modem is an immediate success.

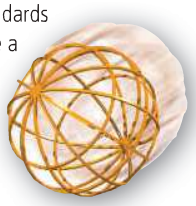
Courtesy of Hewlett-Packard Company

1982 Compaq, Inc. is founded to develop and market IBM-compatible PCs.



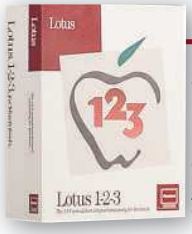
© Cengage Learning

1991 World Wide Web Consortium releases standards that describe a framework for linking documents on different computers.


© Cengage Learning

1982 | 1983 | 1984 | 1986 | 1988 | 1989 | 1991

1983 Instead of choosing a person for its annual award, TIME magazine names the computer Machine of the Year for 1982, acknowledging the impact of computers on society.



© IBM Corporate Archives

1983 Lotus Development Corporation is founded. Its spreadsheet software, Lotus 1-2-3, which combines spreadsheet, graphics, and database programs in one package, becomes the best-selling program for IBM personal computers.


© iStockphoto /audioundwerbung

Apple

1984 Apple introduces the Macintosh computer, which incorporates a unique, easy-to-learn, graphical user interface.


Courtesy of Hewlett-Packard Company

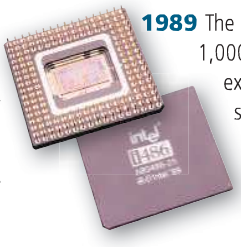
1984 Hewlett-Packard announces the first LaserJet printer for personal computers.

1989 Nintendo introduces the Game Boy, its first handheld game console.


SSPL / The Image Works


Hank Morgan / Science Source

1989 While working at CERN, Switzerland, Tim Berners-Lee invents the World Wide Web.



Courtesy of Intel Corporation

1989 The Intel 486 becomes the world's first 1,000,000 transistor microprocessor. It executes 15,000,000 instructions per second — four times as fast as its predecessor, the 80386 chip.


Courtesy of Microsoft Corporation

1993 Microsoft releases Microsoft Office 3 Professional, the first version of Microsoft Office for the Windows operating system.

Source: amazon.com

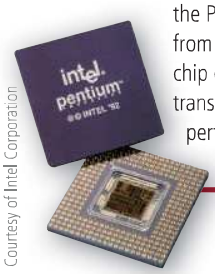
1994 Amazon is founded and later begins business as an online bookstore. Amazon eventually expands to sell products of all types and facilitates the buying and selling of new and used goods. Today, Amazon employs more than 88,400 people.

1995 eBay, an online auction website, is founded. Providing an online venue for people to buy and sell goods, it quickly becomes the world's largest online marketplace as it approaches 100 million active users worldwide.

AP Images/Nigel Treblin/dapd

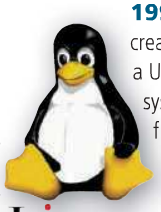
Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners."

1995 Sun Microsystems launches Java, an object-oriented programming language that allows users to write one program for a variety of computer platforms.



Courtesy of Intel Corporation

1993 Several companies introduce computers using the Pentium processor from Intel. The Pentium chip contains 3.1 million transistors and is capable of performing 112,000,000 instructions per second.



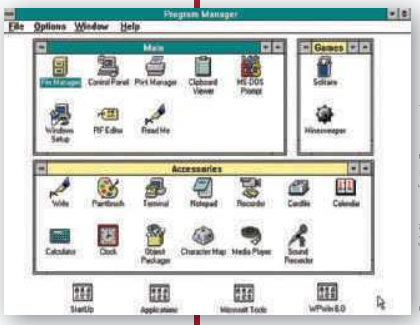
Courtesy of Larry Ewing and The Gimp

1994 Linus Torvalds creates the Linux kernel, a UNIX-like operating system that he releases free across the Internet for further enhancement by other programmers.

/Reuters/Landov

1995 Microsoft releases Windows 95, a major upgrade to its Windows operating system. Windows 95 consists of more than 10,000,000 lines of computer instructions developed by 300 person-years of effort.

1992 | 1993 | 1994 | 1995



Courtesy of Microsoft© Corporation

1992 Microsoft releases Windows 3.1, the latest version of its Windows operating system. Windows 3.1 offers improvements such as TrueType fonts, multimedia capability, and object linking and embedding (OLE). In two months, 3,000,000 copies of Windows 3.1 are sold.

1993 The U.S. Air Force completes the Global Positioning System by launching its 24th Navstar satellite into orbit. Today, GPS receivers can be found in cars, laptops, and smartphones.


Courtesy of Garmin International


© Orhan Cam/ Shutterstock.com

1993 The White House launches its website, which includes an interactive citizens' handbook and White House history and tours.

1994 Jim Clark and Marc Andreessen found Netscape and launch Netscape Navigator 1.0, a browser.

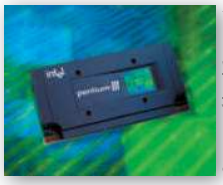
Courtesy of Netscape Communications Corporation

1994 Apple introduces the first digital camera intended for consumers. The Apple QuickTake 100 is connected to home computers using a serial cable.


Courtesy of Mark D. Martin

1994 Yahoo!, a popular search engine and portal, is founded by two Stanford Ph.D. students as a way to keep track of their personal interests on the Internet. Currently, Yahoo! has approximately 11,500 employees in 25 countries, provinces, and territories.

AP Photo/ Paul Sakuma


Courtesy of Intel Corporation

1999 Intel introduces the Pentium III processor. This processor succeeds the Pentium II and can process 3-D graphics more quickly. The Pentium III processor contains between 9.5 and 44 million transistors.

1999 Governments and businesses frantically work to make their computers Y2K (Year 2000) compliant, spending more than $500 billion worldwide.

© Cengage Learning


© Ian Kian Khoon/Shutterstock

1999 Open source software, such as the Linux operating system and the Apache web server created by unpaid volunteers, begins to gain wide acceptance among computer users.

AP Photo

1997 Microsoft releases Internet Explorer 4.0 and seizes a key place in the Internet arena.


Courtesy of Intel Corporation

1997 Intel introduces the Pentium II processor with 7.5 million transistors. The new processor, which incorporates MMX technology, processes video, audio, and graphics data more efficiently and supports programs such as movie editing, gaming, and more.

1996 1997 1998 1999


Courtesy of Palm, Inc.

1996 U.S. Robotics introduces the PalmPilot, an inexpensive user-friendly personal digital assistant (PDA).

1996 Microsoft releases Windows NT 4.0, an operating system for client-server networks.

Box shot reprinted with permission from Microsoft Corporation.

Courtesy of Google, Inc.

1998 Google files for incorporation and is now the most used search engine, capturing more than 60 percent of the market over other search engines.

Brad Cherson / Alamy

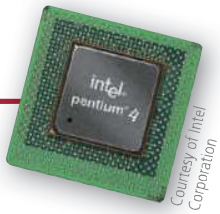
1998 E-commerce booms. Companies such as Amazon.com, Dell, and E*TRADE spur online shopping, allowing buyers to obtain a variety of goods and services.


© Stockphoto/juniorbeep

1998 Apple introduces the iMac, the next version of its popular Macintosh computer. The iMac wins customers with its futuristic design, see-through case, and easy setup.

Source: Napster

2000 Shawn Fanning, 19, and his company, Napster, turn the music industry upside down by developing software that allows computer users to swap music files with one another without going through a centralized file server.



Courtesy of Intel Corporation

2001 Intel unveils its Pentium 4 chip with clock speeds starting at 1.4 GHz. The Pentium 4 includes 42 million transistors.

2002 Digital video cameras, DVD burners, easy-to-use video editing software, and improvements in storage capabilities allow the average computer user to create Hollywood-like videos with introductions, conclusions, rearranged scenes, music, and voice-over.

Courtesy of Intel Corporation

© Cengage Learning

2000 E-commerce achieves mainstream acceptance. Annual e-commerce sales exceed $100 billion, and Internet advertising expenditures reach more than $5 billion.

Wikimedia Foundation

2001 Wikipedia, a free online encyclopedia, is introduced. Additional wikis begin to appear on the Internet, enabling people to share information in their areas of expertise. Although some might rely on wikis for research purposes, the content is not always verified for accuracy.

2002 After several years of negligible sales, the Tablet PC is reintroduced to meet the needs of a more targeted audience.

Courtesy of ViewSonic® Corporation

2000 2001 2002

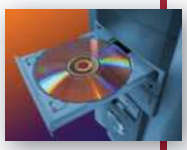
© Cengage Learning

2000 Dot-com (Internet based) companies go out of business at a record pace — nearly one per day — as financial investors withhold funding due to the companies' unprofitability.

Microsoft .net

Source: Microsoft

2002 Microsoft launches its .NET strategy, which is a new environment for developing and running software applications featuring ease of development of web-based services.



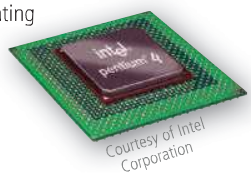
© Tatiana Popova / Shutterstock.com

2002 DVD burners begin to replace CD burners (CD-RW). DVDs can store up to eight times as much data as CDs. Uses include storing home movies, music, photos, and backups.

Kenneth Murray / Science Source

2000 Telemedicine uses satellite technology and videoconferencing to broadcast consultations and to perform distant surgeries. Robots are used for complex and precise tasks.

2002 Intel ships its revamped Pentium 4 chip with the 0.13 micron processor and Hyper-Threading (HT) Technology, operating at speeds of 3.06 GHz. This new development eventually will enable processors with a billion transistors to operate at 20 GHz.



Courtesy of Intel Corporation

2004 Mozilla releases its first version of the Firefox browser. Firefox provides innovative features that enhance the browsing experience for users, including tabbed browsing and a Search box. Firefox quickly gains popularity and takes market share away from Microsoft's Internet Explorer.

AP Photo/screenshot

2004 Companies such as RealNetworks, Microsoft, Sony, and Walmart stake out turf in the online music store business started by Apple.

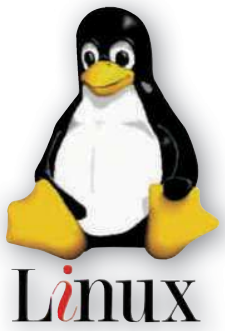
© Cengage Learning

2004 Flat-panel LCD monitors overtake bulky CRT monitors as the popular choice of computer users.

2004 Facebook, an online social network originally available only to college students, is founded. Facebook eventually opens registration to all people and immediately grows to more than 110 million users.

Courtesy of Facebook

2004 Linux, an open source operating system, makes major inroads into the server market as a viable alternative to Microsoft Windows Server 2003, Sun's Solaris, and UNIX.



Courtesy of Larry Ewing and The Gimp

2004 Sony unveils the PlayStation Portable (PSP). This handheld game console is the first to use optical discs.

ISSEI KATO/Reuters/Landov

2004 106 million, or 53 percent, of the 200 million online population in America accesses the Internet via broadband.

2003

© Getty Images

REUTERS/Mannie Garcia / Landov

2003 In an attempt to maintain their current business model of selling songs, the Recording Industry Association of America (RIAA) files more than 250 lawsuits against individual computer users who offer copyrighted music over peer-to-peer networks.

2003 Wireless computers and devices, such as keyboards, mouse devices, home networks, and wireless Internet access points become commonplace.

Courtesy of Palm Inc.

© wavebreakmedia/Shutterstock.com; ©Tom Grill/CORBIS; © iStockphoto /hocus-pocus; © StockLite / Shutterstock.com; ©iStockphoto / Lifesizelmages

2004

2004 USB flash drives become a cost-effective way to transport data and information from one computer to another.

Courtesy of SanDisk Corporation

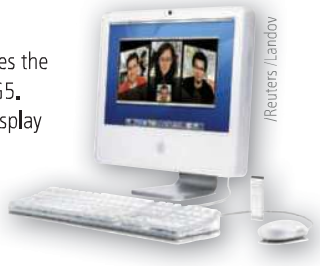
2004 Major retailers begin requiring suppliers to include radio frequency identification (RFID) tags or microchips with antennas, which can be as small as one-third of a millimeter across, in the goods they sell.

Courtesy of Intermec Technologies

Courtesy of Palm Inc.

2004 The smartphone overtakes the PDA as the mobile device of choice.

2004 Apple introduces the sleek all-in-one iMac G5. The new computer's display device contains the system unit.



/Reuters /Landov

2006 Sony launches its PlayStation 3. New features include a Blu-ray Disc player, high-definition capabilities, and always-on online connectivity.

2006 Web 2.0, a term coined in 2004, becomes a household term with the increase in popularity of online social networks, wikis, and web applications.

2005 YouTube, an online community for video sharing, is founded. YouTube includes content such as home videos, movie previews, and clips from television shows. In November 2006, Google acquires YouTube.

Source: YouTube

2006 Apple begins selling Macintosh computers with Intel microprocessors.

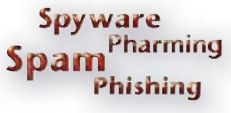
2006 Nintendo releases the Nintendo DS Lite, a handheld game console with new features such as dual screens and improved graphics and sound.

Video iPod

2005 Apple releases the latest version of its popular pocket-sized iPod portable media player. First it played songs, then photos, then podcasts, and now, in addition, up to 150 hours of music videos and television shows on a 2.5" color display.

2005

2006



2005 Spam, spyware, phishing, and pharming take center stage, along with viruses and other malware, as major nuisances to the 801 million computer users worldwide.

2005 Blogging and podcasting become mainstream methods for distributing information via the web.

2005 Microsoft releases the Xbox 360, its latest game console. Features include the capability to play music, display photos, and communicate with computers and other Xbox gamers.

2006 Intel introduces its Core 2 Duo processor family. Boasting record-breaking performance while using less power, the family consists of five desktop computer processors and five mobile computer processors. The desktop processor includes 291 million transistors, yet uses 40 percent less power than the Pentium processor.

2006 IBM produces the fastest supercomputer, Blue Gene/L. It can perform approximately 28 trillion calculations in the time it takes you to blink your eye, or about one-tenth of a second.

2006 Nintendo Wii is introduced and immediately becomes a leader in game consoles. The Wii is being used in revolutionary ways, such as training surgeons.

2007 Intel introduces Core 2 Quad, a four-core processor made for dual-processor servers and desktop computers. The larger number of cores allows for more energy-efficient performance and optimizes battery performance in laptops.

Courtesy of Intel Corporation

2007 VoIP (Voice over Internet Protocol) providers expand usage to include Wi-Fi phones. The phones enable high-quality service through a Wireless-G network and high-speed Internet connection.


Courtesy of Belkin International

2007 Apple releases its Mac OS X version 10.5 "Leopard" operating system, available in a desktop version and server version. The system includes a significantly revised desktop, with a semitransparent menu bar and an updated search tool that incorporates the same visual navigation interface as iTunes.


© oliver leedham /Alamy

2007 Apple introduces the iPhone and sells 270,000 phones in the first 2 days. iPhone uses iTouch technology that allows you to make a call simply by tapping a name or number in your address book. In addition, it stores and plays music like an iPod. Also, Apple sells its one billionth song on iTunes.


© Neville Elder/Corbis

2008 Smartphones become smarter. Smartphones introduced this year include enhanced features such as touch screens with multi-touch technology, mobile TV, tactile feedback, improved graphics, GPS receivers, and better cameras.


AP Photo/Mark Lennihan


Courtesy of Microsoft Corporation

2008 Bill Gates retires from Microsoft. He continues as chairman and advisor on key development projects.

2008 Google releases its new browser. Google Chrome uses an entirely unique interface and offers other features such as dynamic tabs, crash control, and application shortcuts.

Source: Google

2007

2007 Half of the world's population uses mobile phones. More and more people are using a mobile phone in lieu of a landline in their home.


© Sean Locke/iStockphoto

2007 Blu-ray Discs increase in popularity, overcoming and replacing HD DVD in less than one year. A Blu-ray Disc can store approximately 9 hours of high-definition (HD) video on a 50 GB disc or approximately 23 hours of standard-definition (SD) video.


Helene Rogers/Art Directors & Trips Photo/AGE Fotostock

© Rtimages /Shutterstock.com

2007 Wi-Fi hot spots are popular in a variety of locations. People bring their computers to coffeehouses, fast food restaurants, or bookstores to access the Internet wirelessly, either free or for a small fee.

2008

2008 Netflix, an online movie rental company, and TiVo, a company manufacturing digital video recorders (DVRs), make Netflix movies and television episodes available on TiVo DVRs.

Source: Netflix

©1998-2013 TiVo Inc. All rights reserved.

2008 Computer manufacturers begin to offer solid-state drives (SSDs) instead of hard disks, mostly in laptops. Although SSDs have a lower storage capacity, are more expensive, and slightly more susceptible to failure, they are significantly faster.


© Bedo / Dreamstime.com

2008 WiMAX goes live! The advantage of this technology is the capability to access video, music, voice, and video calls wherever and whenever desired. Average download speeds are between 2 Mbps and 4 Mbps. By year's end, Sprint has approximately 100 million users on its network.


iStockphoto

2009 Intel releases the Core i5 and Core i7 line of processors. These processors offer increased performance for some of the more demanding tasks. Intel also enhances its Core processor family by releasing multi-core processors, designed to increase the number of instructions that can be processed at a given time.

2009 Online social networks revolutionize communications. Schools, radio stations, and other organizations develop pages on popular online social networks, such as Facebook, creating closer connections with their stakeholders.

2009 In June 2009, federal law requires that all full-power television stations broadcast only in digital format. Analog television owners are required to purchase a converter box to view over-the-air digital programming.

2009 Computers and mobile devices promote fitness by offering games and programs to help users exercise and track their progress. These games and programs also are used to assist with physical rehabilitation.

Google docs
Source: Google

2009 Web apps continue to increase in popularity. Web apps make it easier to perform tasks such as word processing, photo editing, and tax preparation without installing software on your computer.

2011 Netbooks offer a smaller, lighter alternative to laptops. Netbooks have screens between seven and ten inches, and are used mostly for browsing the web and communicating online.

2011 E-books and e-book readers explode in popularity. Many novels, textbooks, and other publications now are available digitally and can be read on an e-book reader, computer, or mobile device.

2011 More than 200 types of mobile devices are using Google Android, an operating system originally designed for mobile devices.

2011 Steve Jobs, a cofounder of Apple, passes away after a long battle with cancer. Jobs is remembered for revolutionizing the computer and music industries.

2011 A new generation of browsers is released to support HTML5, enabling webpages to contain more vivid, dynamic content.

2009 | 2010 | 2011

2010 Hard disk capacity continues to increase at an exponential rate, with the largest hard disks storing more than 2.5 TB of data and information.

2011 Google introduces its Google+ online social network and integrates it across many of its products and services.

AMD
Source: AMD

2010 AMD develops a 12-core processor, which contains two 6-core processors, each on an individual chip. Power consumption is similar to that of a 6-core processor but offers reduced clock speed.

2010 Apple releases the iPad, a revolutionary mobile device with a 9.7-inch multi-touch screen. The iPad boasts up to 10 hours of battery life, connects wirelessly to the Internet, and is capable of running thousands of apps.

2010 Kinect for Xbox 360 changes the way people play video games. Game players now can interact with the game with a series of sensors, as well as a camera, tracking their movements in 3-D.

2011 Intel introduces Ultrabooks, which are powerful, lightweight alternatives to laptops. Ultrabooks normally weigh three pounds or less, have great performance and battery life, and are usually less than one inch thick.

2012 Microsoft announces the Surface, a tablet designed to compete with Apple's iPad. The Surface has a built-in stand, runs the Windows 8 operating system and its apps, and supports a cover that also can serve as a keyboard.

Source: Microsoft

2012 Microsoft releases Windows 8, its newest version of the Windows operating system. Windows 8 boasts a completely redesigned interface and supports touch input.

2012 Apple releases the iPhone 5. This newest iPhone has a four-inch screen, contains a new, smaller connector, and uses Apple's A6 processor.

Source: Apple

2012 Google's Android surpasses Apple's iOS as the most popular operating system used on smartphones. Although the iPhone still is the bestselling smartphone, competing products are gaining market share quickly.

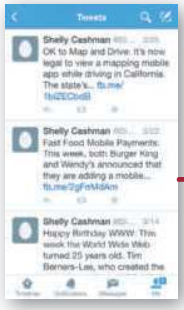
Source: Google

© Cengage Learning

2012 Microsoft releases Office 2013. Office 365, which uses the familiar Office 2013 interface, also is released, allowing users to use their Microsoft accounts to access Office apps from computers that do not have Office installed.

2012 Nintendo releases the Wii U game console.

2013 Twitter users generate more than 500 million Tweets per day.



2013 Sony releases the PlayStation 4 (PS4) game console and Microsoft releases the Xbox One game console.

2013 Amazon announces it will use drones to deliver packages to its customers.

Courtesy of Amazon

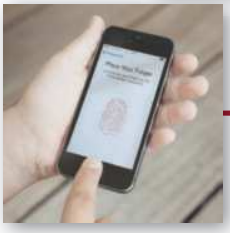
2013 Tablet sales grow at a faster rate than personal computer sales ever grew.

2013 Samsung releases the Galaxy Gear, a smartwatch that synchronizes with a Samsung Galaxy smartphone using Bluetooth technology.

© Ivan Garcia / Shutterstock

2013 Windows 8.1, a significant update to Microsoft's Windows 8 operating system, is released.

Source: Microsoft



© iStockPhoto / Mlenny

2013 Apple releases the iPhone 5S, the first iPhone with TouchID. TouchID verifies a user's identity using an integrated fingerprint reader.

2013 QR codes rapidly gain in popularity, giving mobile device users an easy way to access web content.

Source: qr-code-generator.com

© Stockphoto/mozcann

2013 Many consumers prefer tablets for their mobile computing needs. Tablets provide ultimate portability while still allowing users to access a vast array of apps, as well as access to the Internet and their email messages.

Green Computing

2014 Individuals and enterprises increase their focus on green computing. Computer manufacturers not only sell more energy-efficient hardware, they also provide easy ways in which customers can recycle their old computers and devices.

© Cengage Learning

2014 Solid-state storage is becoming more popular, with storage capacities increasing and prices decreasing.

©Oleksiy Mark /Shutterstock.com

2014 Decreases in storage costs and increases in Internet connection speeds persuade more users to use cloud storage for their data. Cloud storage also provides users with the convenience of accessing their files from almost anywhere.

© Cengage Learning

2014 Apple releases the Apple Watch, a wearable device that runs apps and can monitor various aspects of your health and fitness.

Courtesy of Apple, Inc.

2015 3-D printing decreases in price and increases in popularity.

© dreamnikon / Fotolia

© iStockPhoto / xefstock

2015 Microsoft releases Windows 10, the latest version of its operating system. Windows 10 expands on many of the new features introduced in Windows 8, and also brings back popular features, such as the Start menu, from previous versions of Windows.

2015 Individuals and families are increasingly turning to streaming video on the Internet and abandoning their cable companies.

2014

2014 Bitcoin continues to grow as a digital currency and online payment system.

Courtesy of Mark Frydenberg

2014 Apple releases the iPhone 6 and iPhone 6 Plus. Both devices have significantly larger screens than its predecessors.

Courtesy of Apple, Inc.

2014 Televisions with features such as curved screens and Ultra HD displays begin to increase in popularity.

© iStockPhoto / JazzIRT

© iStockPhoto / ferrantraite

2014 Google Glass goes on sale to the public in the United States.

2014 Amazon drops the price of its Fire Phone to $0.99, possibly indicating that apps and services are valued more than the device.

2015

© iStockPhoto / Ilya_Starikov

2015 Emerging protocols, such as LTE-A and Wi-Fi 802.11 ac, ad, aq, and ah, increase performance on mobile and wireless networks.

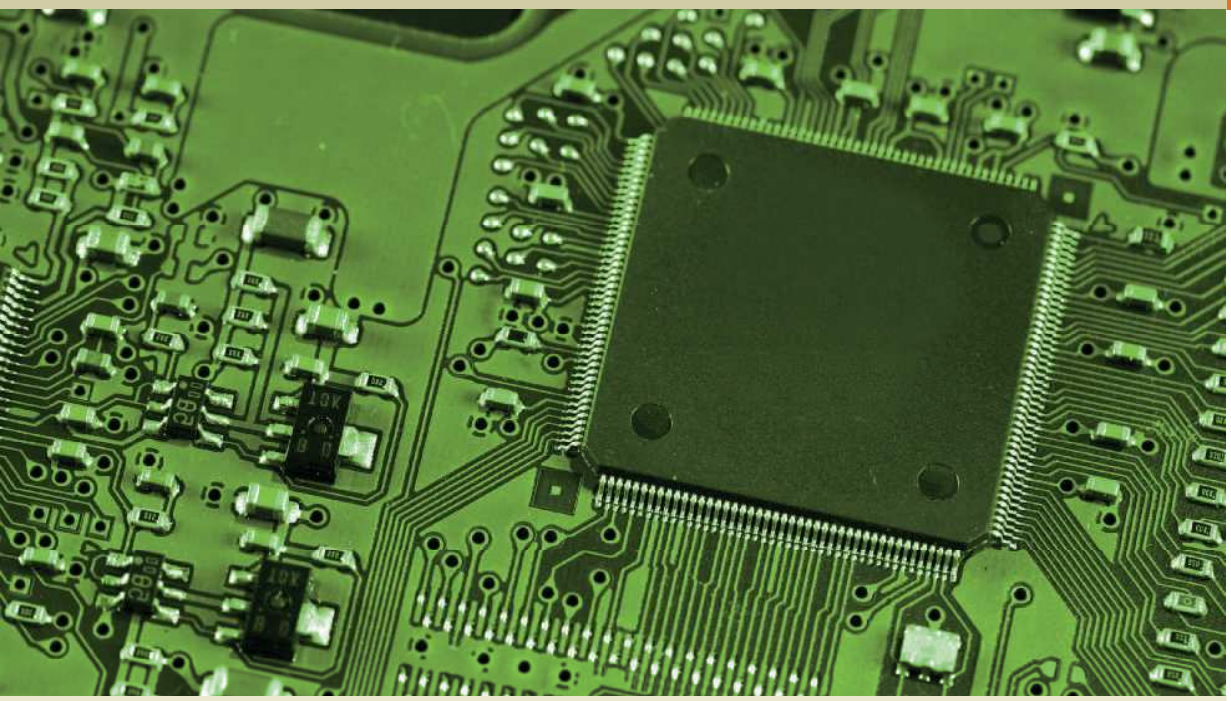
2015 Approximately 91% of all Internet traffic is video, including HD and 3-D video.

2015 Microsoft releases Office 2016, which includes new productivity software and application updates.

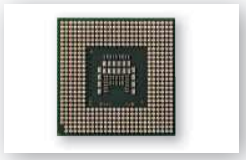
Notes

COMPUTING COMPONENTS:
Processors, Memory, the Cloud, and More

6



Computers and mobile devices contain a variety of electronic components.



"I bought my laptop a couple of years ago, and it appears to be working well. Although at times it runs a little slow and generates a lot of heat, I really have not had problems with it. Why would I need to learn about hardware inside my laptop and other devices?"

While you may be familiar with some of the content in this chapter, do you know how to . . .

- Protect computers and mobile devices from theft?
- Select the right processor?
- Recognize the Internet of Things?
- Make use of cloud computing services?
- Prevent a computer from overheating?
- Determine memory requirements?
- Install memory?
- Erase your mobile phone's memory?
- Familiarize yourself with efforts related to technology products made with fair trade practices?
- Identify which ports you might need on a computer or mobile device?
- Clean a computer or mobile device?
- Conserve battery life on mobile computers and devices?

In this chapter, you will discover how to perform these tasks along with much more information essential to this course. For additional content available that accompanies this chapter, visit the free resources and premium content. Refer to the Preface and the Intro chapter for information about how to access these and other additional instructor-assigned support materials.