

13th
Edition

Understanding Computers

Today and Tomorrow

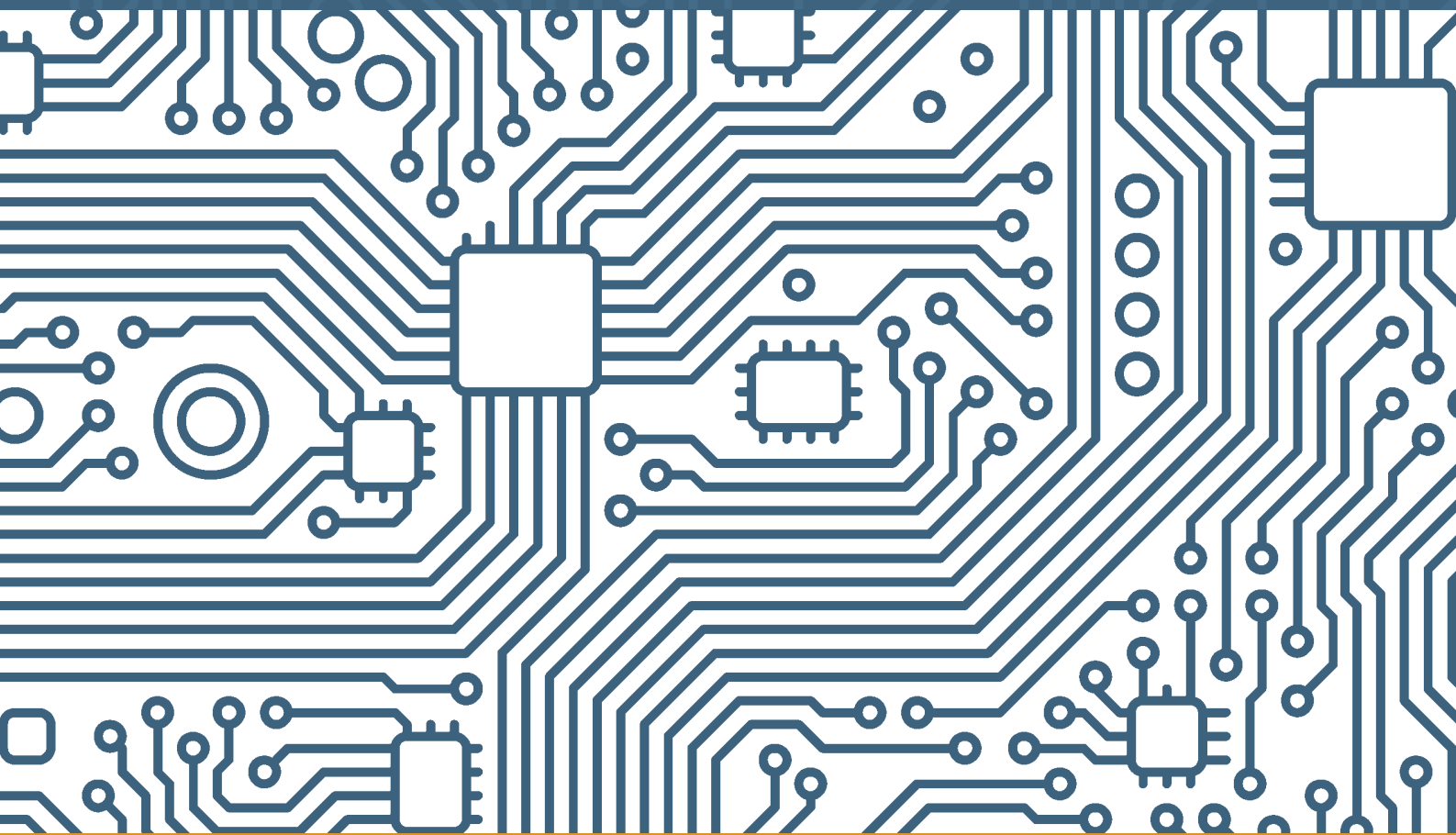
INTRODUCTORY



Deborah Morley • Charles S. Parker

13th Edition

UNDERSTANDING COMPUTERS: TODAY AND TOMORROW



INTRODUCTORY

DEBORAH MORLEY
CHARLES S. PARKER

 **COURSE TECHNOLOGY**
CENGAGE Learning™

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

**Understanding Computers: Today and Tomorrow,
13th Edition****Deborah Morley and Charles S. Parker**

Vice President of Publishing: Nicole Jones Pinard

Executive Editor: Marie Lee

Associate Acquisitions Editor: Brandi Shailer

Product Manager: Katherine C. Russillo

Product Manager: Leigh Heffron

Associate Product Manager: Julia Leroux-Lindsey

Editorial Assistant: Zina Kresin

Senior Marketing Manager: Ryan DeGrote

Marketing Coordinator: Kristen Panciocco

Development Editor: Pam Conrad

Content Project Manager: Heather Hopkins

Print Buyer: Fola Orekoya

Proofreader: Brandy Lilly

Indexer: Elizabeth Cunningham

Composition: Integra Software Services

Text and Cover Designer: Marissa Falco

© 2011 Course Technology, Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product, submit all
requests online at **cengage.com/permissions**

Further permissions questions can be emailed to
permissionrequest@cengage.com

Library of Congress Control Number: 2010920338

Student Edition ISBN 13: 978-0-538-74811-7

Student Edition ISBN 10: 0-538-74811-7

Course Technology

20 Channel Center Street

Boston, MA 02210

USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at:

international.cengage.com/region

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your course and learning solutions, visit **www.cengage.com**

Purchase any of our products at your local college store or at our preferred online store **www.CengageBrain.com**

chapter 9

Network and Internet Security

After completing this chapter, you will be able to do the following:

1. Explain why computer users should be concerned about network and Internet security.
2. List several examples of unauthorized access and unauthorized use.
3. Explain several ways to protect against unauthorized access and unauthorized use, including access control systems, firewalls, and encryption.
4. Provide several examples of computer sabotage.
5. List how individuals and businesses can protect against computer sabotage.
6. Discuss online theft, identity theft, spoofing, phishing, and other types of dot cons.
7. Detail steps an individual can take to protect against online theft, identity theft, spoofing, phishing, and other types of dot cons.
8. Identify personal safety risks associated with Internet use.
9. List steps individuals can take to safeguard their personal safety when using the Internet.
10. Discuss the current state of network and Internet security legislation.

outline

Overview

Why Be Concerned about Network and Internet Security?

Unauthorized Access and Unauthorized Use

- Hacking
- War Driving and Wi-Fi Piggybacking
- Interception of Communications

Protecting Against Unauthorized Access and Unauthorized Use

- Access Control Systems
- Firewalls, Encryption, and Virtual Private Networks (VPNs)
- Additional Public Hotspot Precautions
- Sensible Employee Precautions

Computer Sabotage

- Botnets
- Computer Viruses and Other Types of Malware
- Denial of Service (DoS) Attacks
- Data, Program, or Web Site Alteration

Protecting Against Computer Sabotage

- Security Software
- Other Security Precautions

Online Theft, Online Fraud, and Other Dot Cons

- Theft of Data, Information, and Other Resources
- Identity Theft, Phishing, and Pharming
- Online Auction Fraud
- Other Internet Scams

Protecting Against Online Theft, Online Fraud, and Other Dot Cons

- Protecting Against Data and Information Theft
- Protecting Against Identity Theft, Phishing, and Pharming
- Protecting Against Online Auction Fraud and Other Internet Scams

Personal Safety Issues

- Cyberbullying and Cyberstalking
- Online Pornography

Protecting Against Cyberbullying, Cyberstalking, and Other Personal Safety Concerns

- Safety Tips for Adults
- Safety Tips for Children and Teens

Network and Internet Security Legislation

OVERVIEW

As discussed in the last few chapters, networks and the Internet help many of us be more efficient and effective workers, as well as add convenience and enjoyment to our personal lives. However, there is a downside, as well. The widespread use of home and business networks and the Internet increases the risk of unauthorized computer access, theft, fraud, and other types of computer crime. In addition, the vast amount of business and personal data stored on computers accessible via company networks and the Internet increases the chances of data loss due to crime or employee errors. Some online activities can even put your personal safety at risk, if you are not careful.

This chapter looks at a variety of security concerns stemming from the use of computer networks and the Internet in our society, including unauthorized access and use, computer viruses and other types of sabotage, and online theft and fraud. Safeguards for each of these concerns are also covered, with an explanation of precautions that can be taken to reduce the chance that these security problems will happen to you. Personal safety issues related to the Internet are also discussed, and the chapter closes with a look at legislation related to network and Internet security. ■

WHY BE CONCERNED ABOUT NETWORK AND INTERNET SECURITY?

From a *computer virus* making your computer function abnormally, to a *hacker* using your personal information to make fraudulent purchases, to someone harassing you online in a discussion group, a variety of security concerns related to computer networks and the Internet exist. Many Internet security concerns today can be categorized as **computer crimes**. Computer crime—sometimes referred to as *cybercrime*—includes any illegal act involving a computer. Many computer crimes today are committed using the Internet or another computer network and include theft of financial assets or information, manipulating data (such as grades or account information), and acts of sabotage (such as releasing a computer virus or shutting down a Web server). Cybercrime is an important security concern today. It is a multibillion-dollar business that is often performed by seasoned criminals. In fact, according to the FBI, organized crime organizations in many countries are increasingly turning to computer crime to target millions of potential victims easily, and *phishing attacks* and other *Internet scams* (discussed shortly) are expected to increase in reaction to the recent troubled economy. These and other computer crimes that are carried out via the Internet or another computer network are discussed in this chapter. Other types of computer crime (such as using a computer to create counterfeit currency or make illegal copies of a DVD) are covered in Chapter 15.

PODCAST



Go to www.cengage.com/computerconcepts/np/uc13

to download or listen to the “Expert Insight on Networks and the Internet” podcast.



> **Computer crime.** Any illegal act involving a computer.

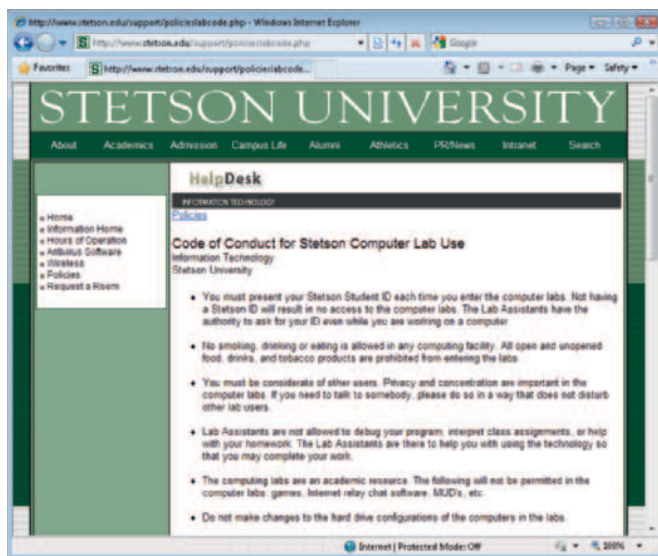
With some security concerns, such as when a spyware program changes your browser's home page, the consequence may be just an annoyance. In other cases, such as when someone steals your identity and purchases items using your name and credit card number, the consequences are much more serious. And, with the growing use of wireless networks, Web 2.0 applications (such as social networking sites), and individuals accessing company networks remotely, paired with an increasing number of security and privacy regulations that businesses need to comply with, network and Internet security has never been more important. Consequently, all computer users should be aware of the security concerns surrounding computer network and Internet use, and they should take appropriate precautions. The most common types of security risks related to network and Internet use, along with some corresponding precautions, are discussed throughout this chapter.

UNAUTHORIZED ACCESS AND UNAUTHORIZED USE

Unauthorized access occurs whenever an individual gains access to a computer, network, file, or other resource without permission—typically by *hacking* into the resource. **Unauthorized use** involves using a computer resource for unauthorized activities. Often, they happen at the same time, but unauthorized use can occur when a user is authorized to access a particular computer or network but is not authorized for the particular activity the user performs. For instance, while a student may be authorized to access the Internet via a campus computer lab, some use—such as viewing pornography—would likely be deemed off-limits. If so, viewing that content from a school computer would be considered unauthorized use. For employees of some companies, checking personal e-mail or visiting personal Facebook pages at work might be classified as unauthorized use.

Unauthorized access and many types of unauthorized use are criminal offenses in the United States and many other countries. They can be committed by both *insiders* (people who work for the company whose computers are being accessed) and *outsiders* (people who do not work for that company). Whether or not a specific act constitutes unauthorized use or is illegal depends on the circumstances, as well as the specific company or institution involved. To explain acceptable computer use to their employees, students, or other users, many organizations and educational institutions publish guidelines for behavior, often called *codes of conduct* (see Figure 9-1). Codes of conduct typically address prohibited activities, such as playing games, installing personal software, violating copyright laws, causing harm to computers or the network, and snooping in other people's files.

FIGURE 9-1
A sample code of conduct.



Hacking

Hacking refers to the act of breaking into a computer or network. It can be performed in person by hacking into a computer the *hacker* has physical access to, but it is more often performed via the Internet or another network. Unless authorized (such as when a company

> **Unauthorized access.** Gaining access to a computer, network, file, or other resource without permission. > **Unauthorized use.** Using a computer resource for unapproved activities. > **Hacking.** Using a computer to break into another computer system.

hires a *professional hacker* to test the security of its system), hacking in the United States and many other countries is a crime.

Typically, the motivation for hacking is to steal data, sabotage a computer system, or perform some other type of illegal act. In particular, the theft of consumer data (such as credit card numbers and cardholder information) has increased dramatically over the past several years—one breach, discovered in 2009, compromised the data of millions of debit and credit cards. Another growing trend is to hack into a computer and “hijack” it for use in an illegal or unethical act, such as generating spam or hosting pornographic Web sites. Hackers are also increasingly aiming attacks at very specific individuals, such as product designers and other individuals who have access to valuable corporate data.

In addition to being a threat to individuals and businesses, hacking is also considered a very serious threat to national security in the United States. The increased number of systems that are controlled by computers and are connected to the Internet, along with the continually improving abilities of hackers and the increasing availability of sets of tools (sometimes called *rootkits*) that allow hackers to access a system, has led to an increased risk of *cyberterrorism*—where terrorists launch attacks via the Internet. Current concerns include attacks against the computers controlling vital systems (such as the nation’s power grids, banks, and water filtration facilities), as well as computers related to national defense, the airlines, and the stock market. In fact, outsiders attempt to access U.S. Pentagon computers millions of times each day, and military leaders are concerned about the potential of cybersecurity threats from other countries. As a result, President Obama has made cybersecurity a priority, including setting up a cybersecurity task force and czar, and stating, “It’s now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation.”

Today, hackers often gain access via a wireless network. This is because wireless networks are becoming increasingly common and it is easier to hack into a wireless network than a wired network. In fact, as discussed in Chapter 7, it is possible to gain access to a wireless network just by being within range (about 100 to 300 feet, depending on the Wi-Fi standard being used) of a wireless access point, unless the access point is sufficiently protected. Although security features are built into wireless routers and other networking hardware, they are typically not enabled by default. As a result, many wireless networks belonging to businesses and individuals—some estimates put the number as high as 70% of all Wi-Fi networks—are left unsecured. Securing a Wi-Fi network is discussed shortly.

ASK THE EXPERT



Moshe Vardi, Rice University, Co-Chair of the ACM Globalization and Offshoring of Software Taskforce

Is there a national security risk to outsourcing/offshoring software development?

Offshoring magnifies existing risks and creates new and often poorly understood threats. When businesses offshore work, they increase not only their own business-related risks (e.g., intellectual property theft) but also risks to national security and to individuals’ privacy. While it is unlikely these risks will deter the growth of offshoring, businesses and nations should employ strategies to mitigate the risks. Businesses have a clear incentive to manage these new risks to suit their own interests, but nations and individuals often have little awareness of the exposures created. For example, many commercial off-the-shelf (COTS) systems are developed offshore, making it extremely difficult for buyers to understand all of the source and application code in the systems. This creates the possibility that a hostile nation or nongovernmental hostile agent (such as a terrorist or criminal) could compromise these systems. Individuals are also often exposed to loss of privacy or identity theft due to the number of business processes being offshored today and managed under laws that are much less restrictive than in most developed countries.

War Driving and Wi-Fi Piggybacking

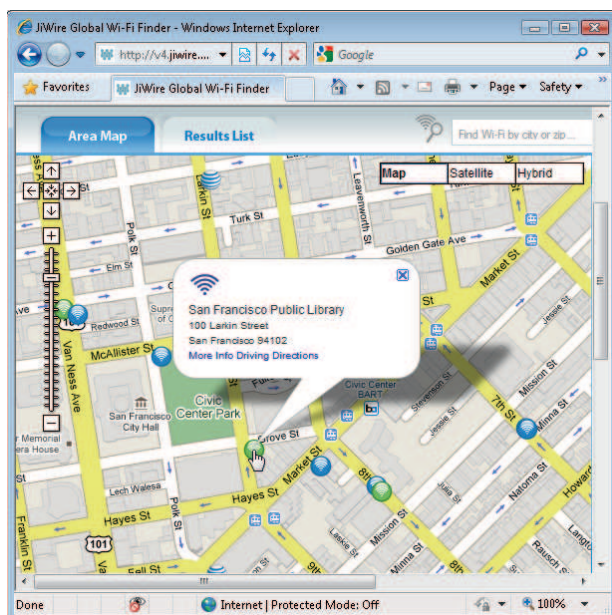
Unauthorized use of a Wi-Fi network is called **war driving** or **Wi-Fi piggybacking**, depending on the location of the hacker at the time. War driving typically involves driving in a car with a portable computer looking for unsecured Wi-Fi networks to connect to. Wi-Fi piggybacking refers to accessing someone else's unsecured Wi-Fi network from the hacker's current location (such as inside his or her home, outside a Wi-Fi hotspot location, or near a local business). Both war driving and Wi-Fi piggybacking are ethically—if not legally—questionable acts. They can also lead to illegal behavior, such as individuals deciding to use data (credit card numbers, for instance) they run across while war driving for fraudulent purposes, as was the case with two men who illegally accessed a Lowe's wireless network during a war drive and later decided to steal credit card numbers via that network. War driving and Wi-Fi piggybacking can also have security risks, both for the hacker and the owner of the Wi-Fi network that is being used. For instance, they both risk the introduction of computer viruses (either intentionally or unintentionally) and unauthorized access of the data located on their computers. In addition, the owner may experience reduced performance or even the cancellation of his or her Internet service if the ISP limits bandwidth or the number of computers allowed to use a single Internet connection.

While there are products and services available to help mobile users locate legitimate public Wi-Fi hotspots (see Figure 9-2), laws in some countries, such as the U.K., are clear that unauthorized access of a Wi-Fi connection is illegal. In the United States, federal law is not as clear, although some states (such as Michigan) have made using a Wi-Fi connection without permission illegal. In fact, a Michigan man was found guilty, fined, and sentenced to community service in 2007 for using the free Wi-Fi service offered to customers at a local café because he was using the service from his parked car located on the street outside the café to check his e-mail on a regular basis.

Advocates of war driving and Wi-Fi piggybacking state that, unless individuals or businesses protect their access points, they are welcoming others to use them. Critics compare that logic to that of an unlocked front door—you cannot legally enter a home just because the front door is unlocked. Some wireless network owners do leave their access points unsecured on purpose and some communities are creating a collection of wireless access points to provide wireless Internet access to everyone in that community. However, it is difficult—if not impossible—to tell if an unsecured network is that way intentionally, unless connecting to the wireless network displays a welcome screen stating that it is a free public Wi-Fi hotspot.

Some feel the ethical distinction of using an unsecured wireless network is determined by the amount of use, believing that it is acceptable to borrow someone's Internet connection to do a quick e-mail check or Google search, but that continually using a neighbor's Internet connection to avoid paying for your own is crossing over the line. Others feel that allowing outsiders to share an Internet connection is acceptable use, as long as the subscriber does not charge the outsider for that access. Still others believe that an Internet connection is intended for use only by the subscriber and that sharing it with others is unfair to the subscriber's ISP. This issue is beginning to be addressed by the courts and

FIGURE 9-2
Wi-Fi finders. Some online mapping services list the Wi-Fi hotspots for a particular geographic area.



> **War driving.** Driving around an area with a Wi-Fi-enabled computer or mobile device to find a Wi-Fi network to access and use without authorization. > **Wi-Fi piggybacking.** Accessing an unsecured Wi-Fi network from your current location without authorization.

ISPs, and some answers regarding the legality of “Wi-Fi borrowing” and Internet connection sharing will likely be forthcoming in the near future. However, the ethical questions surrounding this issue may take longer to resolve.

Interception of Communications

Instead of accessing data stored on a computer via hacking, some criminals gain unauthorized access to data, files, e-mail messages, VoIP calls, and other content as it is being sent over the Internet. For instance, *unencrypted* (unsecured) messages, files, logon information, and more sent over a wireless network (such as while using a public Wi-Fi hotspot or over an unsecured home or business Wi-Fi network) can be captured and read by anyone within range using software designed for that purpose. Once intercepted, the data can be used for unintended or fraudulent purposes.

Although it is unlikely that anyone would be interested in intercepting personal e-mail sent to friends and relatives, proprietary corporate information and sensitive personal information (such as credit card numbers and Web site logon information) is at risk if it is sent unsecured over the Internet or over a wireless home or corporate network. The widespread use of wireless networks, as well as the increased use of wireless connections to transmit data via mobile phones and other portable devices, has opened up new opportunities for data interception. For instance, the data on mobile devices with Bluetooth capabilities enabled can be accessed by other Bluetooth devices that are within range.

A new trend is criminals intercepting credit and debit card information during the card verification process; that is, intercepting the data from a card in real time as a purchase is being authorized. In several recent cases, this occurred via *packetsniffing* software installed at payment terminals (such as restaurant cash registers or gas station credit/debit card readers) by hackers—the packetsniffing software gathered the data during transactions and then sent it to the hackers. The increased occurrence of real-time attacks may be partly because of the new *Payment Card Industry Data Security Standard (PCI DSS)* rules that require companies to limit the credit card data stored on company servers and to *encrypt* the data that is allowed to be stored. Consequently, hackers may be moving away from targeting data stored on company servers and focusing on stealing data in real time during credit card and debit card transactions.

PROTECTING AGAINST UNAUTHORIZED ACCESS AND UNAUTHORIZED USE

The first step in protecting against unauthorized access and unauthorized use is controlling access to an organization’s facilities and computer networks to ensure that only authorized individuals are granted access. In addition, steps need to be taken to ensure that authorized individuals access only the resources that they are supposed to access.

Access Control Systems

Access control systems are used to control access to facilities, computer networks, company databases, individual Web site accounts, and other assets. They can be *identification systems*, which verify that the person trying to access the facility or system is listed as an authorized user, and/or *authentication systems*, which determine whether or not the person attempting access is actually who he or she claims to be. In businesses, access control systems are often integrated into a comprehensive *identity management (IDM) system* designed to manage users’ access to enterprise systems, such as to grant them secure and appropriate access to the systems they are allowed to access in as convenient a manner as possible to the end user. The three most common types of access control systems are discussed next, followed by a discussion of additional considerations for controlling access to wireless networks.

FIGURE 9-3

Passwords.

Passwords are used to log on to computers, networks, Web sites, and other computing resources.

FIGURE 9-4

Strategies for creating good passwords.

Possessed Knowledge Access Systems

A **possessed knowledge access system** is an identification system that requires the individual requesting access to provide information that only the authorized user is supposed to know. *Passwords* and *cognitive authentication systems* fall into this category.

Passwords, the most common type of possessed knowledge, are secret words or character combinations associated with an individual. They are typically used in conjunction with a *username* (often a variation of the person's first and/or last names or the individual's e-mail address). Username/password combinations are often used to restrict access to networks, computers, Web

sites, routers, and other computing resources—the user is granted access to the requested resource only after supplying the correct information. While usernames and e-mail addresses are not secret, passwords are and, for security purposes, typically appear as asterisks or dots as they are being entered so they cannot be viewed (see Figure 9-3). For some applications (such as ATM machines), a *PIN* or *personal identification number*—a secret combination of numeric digits selected by the user—is used instead of a password. Numeric passwords are also referred to *passcodes*.

One of the biggest disadvantages of password-based systems is that passwords can be forgotten. Another disadvantage is that any individual possessing the proper password will be granted access to the system because the system recognizes the password, regardless of whether or not the person using the password is the authorized user, and passwords can be guessed or deciphered by a hacker or a hacker's computer easily if secure password selection strategies are not applied. For example, many hackers are able to access networking hardware and databases because the system administrator passwords for those

resources are still the default passwords (the ones assigned during manufacturing) and so are commonly known; some insiders gain unauthorized access to systems using passwords written down on sticky notes attached to a user's monitor. Consequently, it is important to select passwords that are *strong passwords* but are also easy to remember without writing them down. Strong passwords are passwords that are at least eight characters long; use a combination of letters, numbers, and symbols; and do not form words found in the dictionary or that match the username that the password is associated with. Some strategies for selecting good passwords are listed in Figure 9-4.

A growing trend in possessed knowledge access systems is the use of *cognitive authentication systems* instead of, or in conjunction with, usernames and passwords. Cognitive authentication systems use information that an individual should know or can remember easily.

PASSWORD STRATEGIES

Make the password at least eight characters, if possible. A five-character password can be cracked by a computer program in less than one minute. A ten-character password, in contrast, has about 3,700 trillion possible character permutations and is considerably safer.

Choose passwords that are not in a dictionary—for instance, mix numbers and special characters with abbreviations or unusual words you will remember, but that do not conform to a pattern a computer can readily figure out.

Do not use your name, your kids' or pets' names, your address, your birthdate, or any other public information as your password.

Determine a *passphrase* that you can remember and use corresponding letters and symbols (such as the first letter of each word) for your password. For instance, the passphrase "My son John is five years older than my daughter Abby" could be used to remember the corresponding strong password "Msji5yotMd@".

Do not keep a written copy of the password in your desk or taped to your monitor. If you need to write down your password, create a password-protected file on your computer that contains all your passwords so you can look them up as needed.

Use a different password for your highly sensitive activities (such as online banking or stock trading) than for Web sites that remember your settings or profile (such as online news, auction, shopping, or bookstore sites). If a hacker determines your password on a low-security site (which is easier to break into than a site located on a secure Web server), he or she can use it on an account containing sensitive data if you use the same password on both accounts.

Change your passwords frequently.

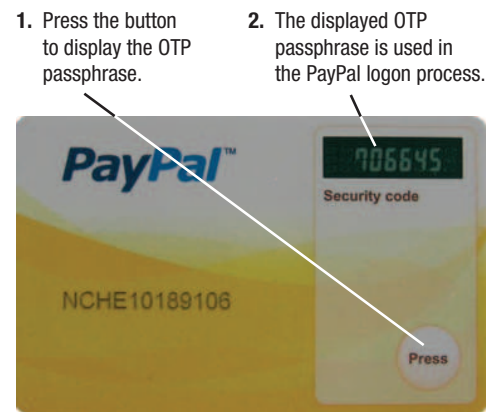
➤ **Possessed knowledge access system.** An access control system that uses information only the individual should know to identify that individual.

➤ **Password.** A secret combination of characters used to gain access to a computer, computer network, or other resource.

Some systems use personal information about the individual (such as his or her city of birth, first elementary school attended, or amount of home mortgage) that was pulled from public databases or the company database and the individual must supply the correct answer in order to be granted access. Other systems (such as the password recovery systems used by many secure Web sites to verify individuals when they forget their password) allow the individual to supply answers to questions when the account is created and then the individual can supply those answers again for authentication purposes when needed.

Possessed knowledge systems are often used in conjunction with the *possessed object access systems* and *biometric access systems* that are discussed next. Using two different methods to authenticate a user is called **two-factor authentication**. Typically, the methods used are some type of possessed knowledge (something you know) along with either a *possessed object* (something you have) or a *biometric feature* (something you are). Two-factor authentication adds an additional level of security to an access control system, since hackers are much less likely to be able to gain access to two different required factors. One emerging type of two-factor authentication used to protect access to sensitive online accounts (such as online banking accounts) uses a conventional username/password combination in conjunction with an access card (such as the one shown in Figure 9-5) that displays a *one-time password (OTP)* when the button on the card is pressed. The OTP changes each time the button is pressed and the current OTP must be entered on the logon screen along with the username/password in order to log on to the account. Two-factor authentication systems are common in many countries and use is growing in the United States. In fact, a federal guideline that went into effect in 2007 instructs banks, credit unions, and other financial institutions to replace single-factor authentication systems (typically username/password systems) with systems using two-factor authentication, and some banks (such as Bank of America) offer two-factor authentication protection via an OTP access card or an OTP sent on demand to your mobile phone. Many other countries are considering or implementing similar guidelines or mandates.

FIGURE 9-5
Two-factor authentication. With this system, the user must have both the access card (to obtain the OTP) and his or her conventional username/password combination, in order to log on to his or her online account.



NET

CAUTION CAUTION CAUTION CAUTION CAUTION CAUTION CAUTION

Don't supply answers to the cognitive authentication questions (like your high school or your pet's name) used in the password recovery process of many Web sites that a hacker may be able to guess based on information found on your Facebook page, an online database, or another online source. Instead, supply answers that you can remember but that also follow secure password rules. For instance, if your dog's name is Spot, you could enter *MDN1s\$pOT* as the answer to a question about your pet's name and remember it as "My dog's name is Spot."

Possessed Object Access Systems

Possessed object access systems use physical objects for identification purposes and they are frequently used to control access to facilities and computer systems. Common types of possessed objects are smart cards, RFID-encoded badges, and magnetic cards that are swiped through or placed close to a reader to be read (see Figure 9-6). Increasingly, *USB security keys* (also called *USB security tokens*)—USB flash drives that are inserted into a computer to grant access to a network, to supply Web site usernames and passwords, or

>Two-factor authentication. Using two different methods to authenticate a user. **>Possessed object access system.** An access control system that uses a physical object an individual has in his or her possession to identify that individual.

**SMART CARDS**

Are read by a smart card reader to provide access to a facility or computer system.

**USB SECURITY TOKENS**

Are inserted into one of the computer's USB ports to provide access to that computer system.

FIGURE 9-6
Possessed objects.
 Help protect against unauthorized access; some can also store additional security credentials.

TIP

Cuts or other changes to a finger may prevent access via a fingerprint reader. To avoid this problem, be sure to enroll more than one finger, if possible, whenever you are being set up in a system that uses a fingerprint reader. Many systems allow the user to enter images for more than one finger and any of the registered fingers may be used for access.

This latter disadvantage can be overcome by using a second factor, such as requiring the user to supply a username/password combination or be authenticated by a fingerprint or other type of *biometric* data in order to use the possessed object.

Biometric Access Systems

Biometrics is the study of identifying individuals using measurable, unique physiological or behavioral characteristics. **Biometric access systems** typically identify users by a particular unique biological characteristic (such as a fingerprint, a hand, a face, or an iris), although personal traits are used in some systems. For instance, some systems today use *keystroke dynamics* to recognize an individual's unique typing pattern to authenticate the user as he or she types in his or her username and password; other systems identify an individual via his or her voice, signature, or gait. Because the means of access (usually a part of the body) cannot typically be used by anyone other than the authorized individual, biometric access systems can perform both identification and authentication.

To identify and authenticate an individual, biometric access systems typically use a biometric reader (such as a *fingerprint reader* or *hand geometry reader* to identify an individual based on his or her fingerprint or hand image) or a digital camera (to identify an individual based on his or her face or iris), in conjunction with software and a database. The system matches the supplied biometric data with the biometric data that was stored in the database when the individual was enrolled in the system and authenticates the individual if the data matches. To speed up the process, many biometric access systems require users to identify themselves first (such as by entering a username or swiping a smart card), and then the system uses that identifying information to verify that the supplied biometric data matches the identified person.

Biometric access systems are used to control access to secure facilities (such as corporate headquarters and prisons); to log users on to computers, networks, and secure Web sites (by using an external reader or one built into the computer); to punch employees in and out of work; and to confirm consumers' identities at ATM machines and check-cashing services. Biometric readers are also increasingly being built into notebook computers, external hard drives (like the one shown in Figure 4-20 in Chapter 4), USB flash drives, and other hardware to prevent unauthorized use of those devices.

to provide other security features—are also being used. Access cards (like the one shown in Figure 9-5) and other devices used to supply the OTPs used to log on to Web sites and other resources are another type of *security token* possessed object.

One disadvantage of using possessed objects is that the object can be lost or, like passwords, can be used by an unauthorized individual if that individual has possession of the object.

**ONLINE VIDEO**

Go to the Chapter 9 page at www.cengage.com/computerconcepts/np/uc13 to watch the "How the Eikon Personal Biometric Reader Works" video clip.

➤ **Biometric access system.** An access control system that uses one unique physical characteristic of an individual (such as a fingerprint, face, or voice) to authenticate that individual.

In addition to being used to control access to computers, networks, and other resources, biometrics are an important part of the systems used by law enforcement agencies and the military to identify individuals. For instance, the border control systems in many countries use biometrics to identify citizens, travelers, criminal suspects, and potential terrorists, and biometric identification systems are used extensively by law enforcement agencies and the military in areas of conflict. For example, biometric identification systems are being used in Iraq to identify members of the Iraqi police and military, prisoners, prison guards, authorized gun owners, citizens, contract employees, known criminals, and criminal suspects. In addition, *face recognition systems* (biometric systems that use cameras and a database of photos to attempt to identify individuals as they walk by the cameras) are used in many airports and other public locations to help identify known terrorists and criminal suspects.

Biometric access systems are very accurate. In fact, the odds of two different individuals having identical irises is 1 in 10^8 and the statistical probability of two different irises being declared a match are 1 in 1.2 million—even identical twins (who have the same DNA structure) have different fingerprints and irises. Systems based on biological characteristics (such as a person's iris, hand geometry, face, or fingerprint) tend to be more accurate than those based on a personal trait (such as a person's voice or written signature) because biological traits do not change, but physical traits might change (such as an individual's voice, which might be affected by a cold, or a written signature, which might be affected by a broken wrist). In addition, biometric characteristics cannot be lost (like an access card), cannot be forgotten (like a password), and do not have to be pulled out of a briefcase or pocket (like an access card or other type of possessed object).

The primary disadvantages of biometric access systems are that much of the necessary hardware and software is expensive, and the data used for authentication (such as a fingerprint or an iris image) cannot be reset if it is compromised. In addition, fingerprint and hand geometry systems typically require contact with the reader device, though some systems under development (such as one that identifies individuals based on the veins in their hands) are contactless systems.

Some examples of the most commonly used types of biometric access and identification systems are shown in Figure 9-7.



FINGERPRINT RECOGNITION SYSTEMS

Typically used to protect access to office computers, to automatically supply Web site passwords on home computers, and to pay for products or services.



FACE RECOGNITION SYSTEMS

Typically used to control access to highly secure areas, as well as to identify individuals for law enforcement purposes.



HAND GEOMETRY SYSTEMS

Typically used to control access to facilities (such as government offices, prisons, and military facilities) and to punch in and out of work.



IRIS RECOGNITION SYSTEMS

Typically used to control access to highly secure areas and by the military; also beginning to be used to authenticate ATM users and other consumers.

FIGURE 9-7
Types of biometric access and identification systems.

VIDEO PODCAST

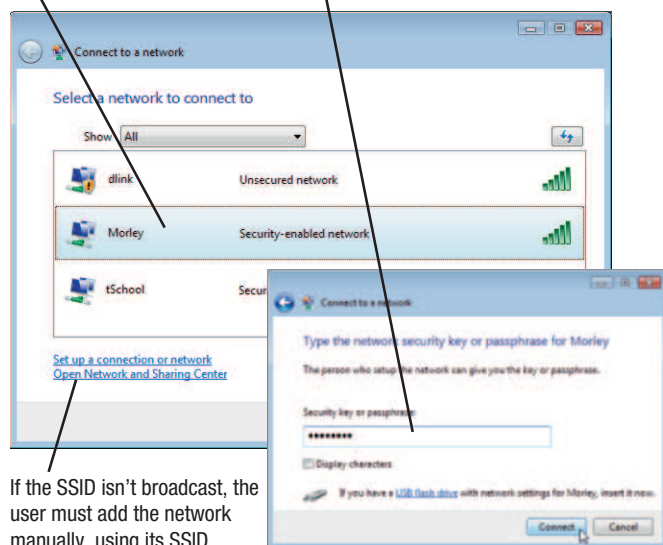
Go to the Chapter 9 page at www.cengage.com/computerconcepts/np/uc13 to download or listen to the "How To: Use Face Recognition with Your Computer" video podcast.

Controlling Access to Wireless Networks

As already discussed, wireless networks—such as Wi-Fi networks—are less secure, in general, than wired networks. There are Wi-Fi security procedures, however, that can be used to protect against unauthorized use of a wireless network and to *encrypt* data sent over the network so that it is unreadable if it is intercepted. The original Wi-Fi security standard was

Because the SSID is being broadcast, the user can select the network from the list.

The user must supply the appropriate network key or passphrase in order to connect to the network.



If the SSID isn't broadcast, the user must add the network manually, using its SSID, in order to log on.

FIGURE 9-8
Accessing a Wi-Fi network. To access a secure network, the appropriate passphrase must be supplied.

WEP (*Wired Equivalent Privacy*). WEP is now considered insecure and has been replaced with the more secure WPA (*Wi-Fi Protected Access*) and the even more secure WPA2 standards. However, Wi-Fi security features only work if they are enabled. Most Wi-Fi hardware today is shipped with the security features switched off, and many network owners never enable them, leaving those networks unsecured.

To protect against unauthorized access, Wi-Fi network owners should secure their networks by changing the router or access point settings to enable one of the encryption standards and to assign a *network key* or *passphrase* (essentially a password) that must be supplied in order to access the secured network. In addition, the name of the network (called the *SSID*) can be hidden from view by switching off the SSID broadcast feature. While hiding the network name will not deter serious hackers, it may reduce the number of casual war drivers or neighbors accessing the network. Once a network is secured, users who want to connect to that network need to either select or supply the network SSID name (depending on whether or not the SSID is being broadcast) and then enter the network key assigned to that network (see Figure 9-8). For an overview of how you can secure your wireless home router, see the *How It Works* box.

Firewalls, Encryption, and Virtual Private Networks (VPNs)

In addition to the access control systems just discussed, there are a number of other tools that can be used to prevent access to an individual computer or to prevent data from being intercepted in an understandable form during transit. These tools are discussed next.

Firewalls

A **firewall** is a security system that essentially creates a barrier between a computer or network and the Internet in order to protect against unauthorized access. Firewalls are typically two-way, so they check all incoming (from the Internet to the computer or the network) and outgoing (from the computer or the network to the Internet) traffic and allow only authorized traffic to pass through the firewall. *Personal firewalls* are typically software-based systems that are geared toward protecting home computers from hackers attempting to access those computers through their Internet connections. All computers with direct Internet connections (such as DSL, cable, satellite, or fixed wireless Internet access) should use a firewall (computers using dial-up Internet access only are relatively safe from hackers). Personal firewalls can be stand-alone programs (such as the free *ZoneAlarm* program); they are also built into many operating systems (such as the *Windows Firewall* program shown in Figure 9-9). Many routers, modems, and other pieces of networking hardware also include built-in firewall capabilities to help secure the networks these devices are used with. Firewalls designed to protect business networks may be software-based, hardware-based, or a combination of the two. They can typically be used both to prevent network access by hackers and other outsiders, as well as to control employee Internet access.

TIP

If a legitimate application installed on your computer needs to access the Internet but cannot, check your firewall settings—you may need to unblock that program.

> **Firewall.** A collection of hardware and/or software intended to protect a computer or computer network from unauthorized access.

HOW IT WORKS

Securing a Wireless Home Router

If you have a home wireless network, it is important to secure it properly so it cannot be used by unauthorized individuals. Security settings are specified in the router's configuration screen, such as the one shown in the accompanying illustration. To open your router's configuration screen to check or modify the settings, type the IP address assigned to that device (such as 192.168.0.1—check for a sticker on the bottom of your router or your router's documentation for its default IP address and username) in your browser's Address bar. Use the default password listed in your router documentation to log on the first time, and then change the password using the configuration screen to prevent unauthorized individuals from changing your router settings. To secure the router, enter the network name (SSID) you want to have associated with the router, select the appropriate security mode (such as WEP, WPA, or WPA2) to be used, and then type a secure passphrase to be used in order to log on to the network.

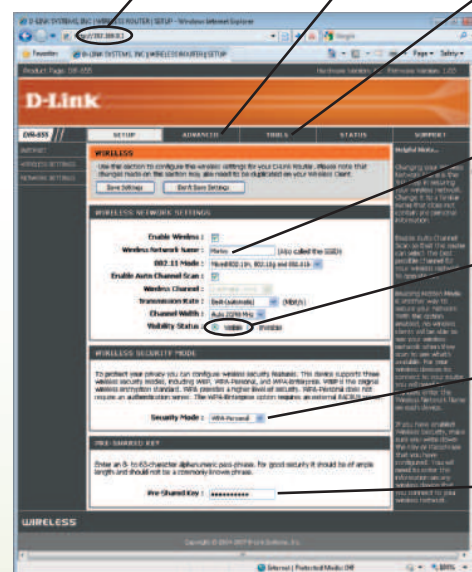
For additional security, *MAC (Media Access Control) address filtering* can be used to allow only the devices whose network adapter MAC addresses you enter into your router's settings access to the network. Because hackers can “spoof” MAC addresses by changing the MAC addresses of their devices to match an authorized MAC address (once the hacker determines those addresses), MAC address filtering should not be considered an alternative to using WPA or WPA2 encryption. However, it does add another layer of protection. Other

precautions include designating specific times (such as when you are away from home) that the router will deny access to any device, and reducing the strength of the wireless signal if its current strength reaches farther than you need.

Use the router's IP address to display the router's configuration screen.

Use this tab to enable MAC address filtering.

Use this tab to change the administrator password used to access this configuration screen.



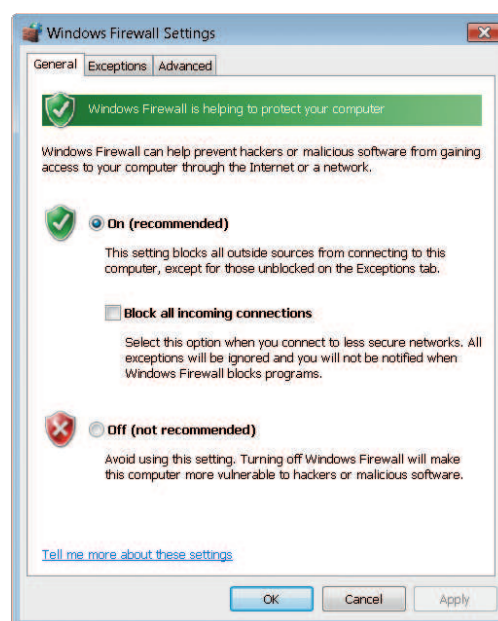
Type your desired SSID here.

Enable SSID broadcast here.

Select the desired security mode here.

Type your desired network key here.

Firewalls work by closing down all external *communications port addresses* (the electronic connections that allow a computer to communicate with other computers) to unauthorized computers and programs. While business firewalls are set up by the network administrator and those settings typically cannot be changed by end users, individuals may choose to change the settings for their personal firewall. For example, the user can choose to be notified when any application program on the computer is trying to access the Internet, to specify the programs that are allowed to access the Internet, or to block all incoming connections temporarily. In addition to protecting your computer from outside access, firewall programs also protect against



ONLINE VIDEO

Go to the Chapter 9 page at www.cengage.com/computerconcepts/np/uc13 to watch the “Securing Your Wireless Router” video clip.

FIGURE 9-9
A personal firewall program. The firewall is on, so only authorized traffic can access the computer.



FIGURE 9-10
Online security scans can check your system for vulnerabilities.

TIP

Sensitive information (such as credit card numbers, account numbers, and Web site passwords) should only be entered on secure Web pages to prevent that data from being intercepted by a criminal.

TIP

An emerging encryption standard that may eventually replace SSL is *Transport Layer Security (TLS)*.

any spyware, computer viruses, or other malicious programs located on your computer that are designed to send data from your computer (such as credit card numbers, Web site passwords, and other sensitive data stored on your hard drive) to a hacker at the hacker's request.

A related type of security system increasingly being used by businesses today is an *intrusion prevention system (IPS)*. Whereas a firewall tries to block unauthorized traffic, an IPS continuously monitors and analyzes the traffic allowed by the firewall to try to detect possible attacks as they are occurring. If an attack is in progress, IPS software can immediately block it.

After installing and setting up a firewall (and an IPS if needed), individuals and businesses should test

their systems to determine if vulnerabilities still exist. Individuals can use online security tests—such as the *Symantec Security Check* shown in Figure 9-10 or the tests at Gibson Research's *Shields Up* site—to check their computers; businesses may wish to hire an outside consultant to perform a comprehensive security assessment.

Encryption

Encryption is a way of temporarily converting data into a form, known as a *cipher*, which is unreadable until it is *decrypted* (unscrambled) in order to protect that data from being viewed by unauthorized individuals. As previously discussed, secure Wi-Fi networks use encryption to secure data that is transferred over the network. **Secure Web pages** use encryption so that sensitive data (such as credit card numbers) sent via the Web page is protected as it travels over the Internet. The most common security protocols used with secure Web pages are *Secure Sockets Layer (SSL)* and *Extended Validation Secure Sockets Layer (EV SSL)*. The URL for Web pages using either form of SSL begins with *https*: instead of *http*:

Some Internet services (such as *Skype VoIP* calls and *HushMail* Web-based e-mails) use built-in encryption. Encryption can also be added manually to a file or an e-mail message before it is sent over the Internet to ensure that the content is unreadable if the file or message is intercepted during transit. In addition to securing files during transit, encryption can be used to protect the files stored on a hard drive so they will be unreadable if opened by an unauthorized person (such as if a hacker accesses a file containing sensitive data or if a computer containing sensitive files is lost or stolen). Increasingly, computers and hard drives (particularly those used with portable computers) are *self-encrypting*; that is, encrypting all data automatically and invisibly to the user. Windows, Mac OS, and other current operating systems support encryption and businesses are increasingly turning to encryption to prevent data loss, if a data breach should occur.

➤ **Encryption.** A method of scrambling the contents of an e-mail message or a file to make it unreadable if an unauthorized user intercepts it.

➤ **Secure Web page.** A Web page that uses encryption to protect information transmitted via that Web page.

The two most common types of encryption in use today are *public key encryption* (often used with content being transmitted over the Internet, such as secure Web pages and encrypted e-mail) and *private key encryption* (most often used to encrypt files or the content of a hard drive or other device). **Private key encryption**, also called *symmetric key encryption*, uses a single secret *private key* (essentially a password) to both encrypt and decrypt the file or message. It is often used to encrypt files stored on an individual's computer, since the individual who selects the private key is likely the only one who will need to access those files. Private key encryption can also be used to send files securely to others, provided both the sender and recipient agree on the private key that will be used to access the file. Private key encryption capabilities are incorporated into a variety of programs today, including Microsoft Office, the WinZip file compression program, and Adobe Acrobat (the program used to create PDF files). To encrypt a document in Microsoft Word, for instance, you use the *Prepare* option on the Office menu, choose *Encrypt Document*, type the desired password (private key), and then save the file. To open that document again (or any copies of the file, such as those sent via e-mail), the password assigned to that file must be entered correctly.

Public key encryption, also called *asymmetric key encryption*, utilizes two encryption keys to encrypt and decrypt documents. Specifically, public key encryption uses a pair of keys (a private key and a *public key*) that are related mathematically to each other and have been assigned to a particular individual. An individual's public key is not secret and is available for anyone to use, but the corresponding private key is used only by the individual to whom it was assigned. Documents or messages encrypted with a public key can only be decrypted with the matching private key.

Public/private key pairs are generated by the program being used to perform the encryption or they are obtained via the Internet through a *Certificate Authority*, such as VeriSign or Thawte. Once obtained, encryption keys are stored in your browser, e-mail program, and any other program with which they will be used—this is typically done automatically for you when you obtain your key pairs. Obtaining a business public/private key pair usually requires a fee, but free key pairs for personal use are available through some Certificate Authorities. If a third-party encryption program is used (such as *Pretty Good Privacy* or *PGP*), the program typically takes care of obtaining and managing your keys for you.

To send someone an encrypted e-mail message or file using public key encryption, you need his or her public key. If that person has previously sent you his or her public key (such as via an e-mail message), it was likely stored by your e-mail program in your address book or contacts list, or by your encryption program in a central key directory used by that program. In either case, that public key is available whenever you want to send that person an encrypted document. If you do not already have the public key belonging to the individual to whom you wish to send an encrypted e-mail or file, you will need to request it from that individual. Once the recipient's public key has been used to encrypt the file or e-mail message and that document is received, the recipient uses his or her private key to decrypt the encrypted contents (see Figure 9-11).

To avoid the need to obtain the recipient's public key before sending that person an encrypted e-mail, *Web-based encrypted e-mail* can be used. Web-based encrypted e-mail works similarly to regular Web-based e-mail (in which e-mail is composed and viewed on a Web page belonging to a Web-based e-mail provider), but Web-based encrypted e-mail systems use secure Web servers to host the Web pages that are used to compose and read e-mail messages. Some Web-based encrypted e-mail systems—such as the popular free *HushMail* service that automatically encrypts all e-mail sent through the

VIDEO PODCAST



Go to the Chapter 9 page at www.cengage.com/computerconcepts/np/uc13 to download or listen to the "How To: Create an Encrypted Partition On Your Hard Drive" video podcast.

NET

FURTHER EXPLORATION

Go

Go to the Chapter 9 page at www.cengage.com/computerconcepts/np/uc13 for links to information about encryption.

>**Public key encryption.** A type of encryption that uses key pairs to encrypt and decrypt the file or message. >**Private key encryption.** A type of encryption that uses a single key to encrypt and decrypt the file or message.

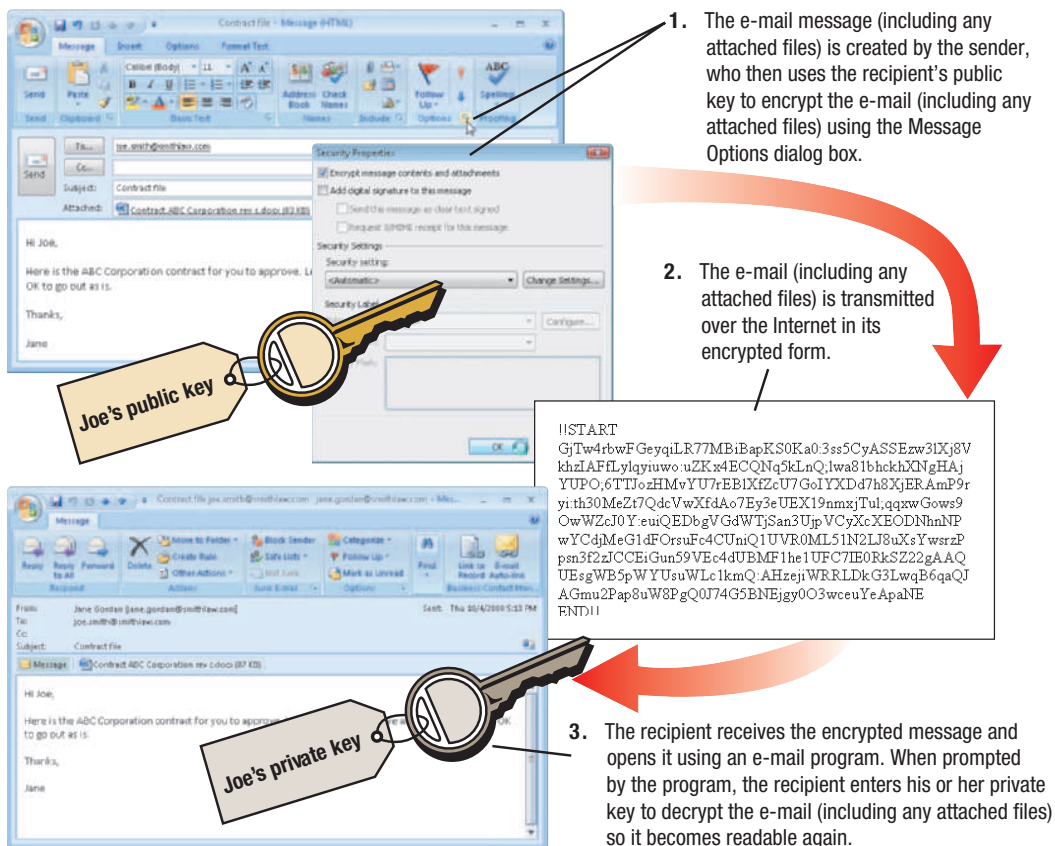


FIGURE 9-11
Using public key encryption to secure an e-mail message.

TIP

Unless it is absolutely necessary and you are using a VPN, do not perform sensitive transactions (such as shopping or banking) at a public hotspot.

service—require both the sender and recipient to have accounts. Others require only the sender to have an account and the recipient is sent an e-mail containing instructions regarding how to view the message on a secure Web page.

There are various strengths of encryption available; the stronger the encryption, the more difficult it is to crack. Older 40-bit encryption (which can only use keys that are 40 bits or 5 characters long) is considered *weak encryption*.

Stronger encryption is available today, such as *strong 128-bit encryption* (which uses 16-character keys) and *military-strength 2,048-bit encryption* (which uses 256-character keys), although not without some objections from law enforcement agencies and the government because they state that terrorists routinely use encryption methods to communicate.

Virtual Private Networks (VPNs)

While e-mail and file encryption can be used to transfer individual messages and files securely over the Internet, a **virtual private network (VPN)** is designed to be used when a continuous secure channel over the Internet is needed. A VPN provides a secure private tunnel from the user's computer through the Internet to another destination and is most often used to provide remote employees with secure access to a company network. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the remote network and that the data cannot be intercepted during transit. Since it uses the Internet instead of an expensive private physical network, a VPN can provide a secure environment over a large geographical area at a manageable cost. Once a VPN is set up, the user just needs to log on (such as with a username/password combination or a security token) in order to use the VPN.

VPNs are often used by both businesses and individuals at public Wi-Fi hotspots to prevent data interception when connecting to the Internet via the hotspot. While businesspeople will typically use a VPN set up by their companies, individuals can create *personal VPNs* using software designed for that purpose. This software automatically encrypts all inbound and outbound Internet traffic, including Web pages, e-mail messages, IMs, VoIP calls, and

>Virtual private network (VPN). A private, secure path over the Internet that provides authorized users a secure means of accessing a private network via the Internet.

so forth, and also acts as a personal firewall. Using a personal VPN at a public hotspot can help individuals from becoming the victim of a growing trend—*evil twin* Wi-Fi access points, discussed in the Trend box.

Additional Public Hotspot Precautions

The precautions already discussed (such as using firewall software, secure Web pages, VPNs, and encryption) are a good start for protecting against unauthorized access and unauthorized use at a public Wi-Fi hotspot. However, there are additional precautions individuals can use to avoid data (both that which is on their computers and that which is being sent over the Internet) from being compromised. These precautions are listed in Figure 9-12.

Sensible Employee Precautions

A significant number of business security breaches—over 60%, according to a recent University of Washington study—are the responsibility of insiders. Sometimes the employee deliberately performs the act; other times the employee makes a mistake, such as losing a portable computer or removable storage medium, or inadvertently providing access to sensitive data. Consequently, it pays for employers to be cautious with their employees. Some suggestions to avoid security breaches by employees are listed next.

Screen Potential New Hires Carefully

Employers should carefully investigate the background of all potential employees. Some people falsify résumés to get jobs. Others may have criminal records or currently be charged with a crime. One embarrassing mistake made by Rutgers University was to hire David Smith, the author of the *Melissa* computer virus, as a computer technician when he was out on bail following the arrest for that crime.

Watch for Disgruntled Employees and Ex-Employees

The type of employee who is most likely to commit a computer crime is one who has recently been terminated or passed over for a promotion, or one who has some reason to want to “get even” with the organization. Limiting access for each employee to only the resources needed for his or her job (referred to as the *Principle of Least Privilege*) and monitoring any attempts to access off-limit resources can help prevent some types of problems, such as unauthorized access of sensitive files, unintentional damage like deleting or changing files inadvertently, or sabotage like deleting or changing company files intentionally. In addition, it is vital that whenever an employee leaves the company for any reason, all access to the system for that individual (username, password, e-mail address, and so forth) should be removed immediately. For employees with high levels of system access, simultaneously removing access while the termination is taking place is even better. Waiting even a few minutes can be too late, since just-fired employees have been known to barricade themselves in their office immediately after being terminated in order to change passwords, sabotage records, and perform other malicious acts. Some wait slightly longer, such as one computer administrator at a Houston organ and tissue donation center who recently pled guilty to accessing the company computer system the evening of and day after being fired and intentionally deleting numerous software applications and important files, such as organ donation records, accounting files, and backup files. She was charged with one

PUBLIC HOTSPOT PRECAUTIONS

Turn off automatic connections and pay attention to the list of available hotspots to try to make sure you connect to a legitimate access point (not an evil twin).

Use a personal firewall to control the traffic going to and from your computer and temporarily use it to block all incoming connections.

Use a virtual private network (VPN) to secure all activity between your computer and the Internet.

Only enter passwords, credit card numbers, and other data on secure Web pages using a VPN.

If you're not using a VPN, encrypt all sensitive files before transferring or e-mailing them.


If you're not using a VPN, avoid online shopping, banking, and other sensitive transactions.

Turn off file sharing so others can't access the files on your hard drive.

Turn off Bluetooth and Wi-Fi when you are not using them.

Disable *ad hoc* capabilities to prevent another computer from connecting to your computer directly without using an access point.

Use antivirus software and make sure your operating system is up to date.

 **FIGURE 9-12**
Sensible precautions for public Wi-Fi hotspot users.

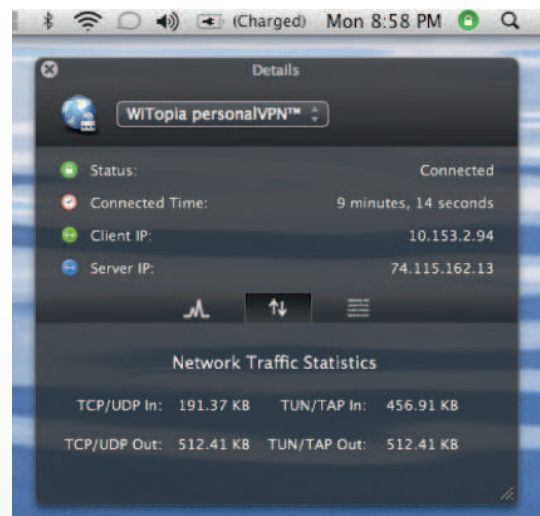
TREND

Evil Twins

An *evil twin* is a fake Wi-Fi hotspot set up by a thief to masquerade as a legitimate Wi-Fi hotspot in order to gather personal or corporate information from individuals who connect to that hotspot thinking it is the legitimate one. Typically, the thief selects a legitimate hotspot and moves within range of that hotspot, uses software to discover the network name (SSID) and radio frequency being used by the legitimate hotspot, and then broadcasts his or her hotspot using the same SSID as the legitimate one. To the end user, the evil twin looks like the legitimate hotspot because it uses the same SSID and settings as the “good twin” it is impersonating. If an end user connects to the evil twin to access the Internet, the thief can intercept sensitive data sent to the Internet, such as passwords or credit card information. That information can then be used for *identity theft* and other fraudulent activities.

Because of the increased use of Wi-Fi hotspots and the availability of software enabling a would-be thief to set up an evil twin hotspot, evil twins are an increasing threat. To make matters worse, some evil twins are able to disconnect users from the legitimate hotspot in hopes the users will be reconnected automatically to the evil twin instead of the legitimate hotspot. To protect yourself, set up your portable computer to only connect manually to hotspots so you cannot be connected to an evil

twin hotspot inadvertently. In addition, refrain from performing sensitive transactions (such as shopping and banking) at public hotspots. Businesspeople should use a VPN when connecting to the company server via a Wi-Fi hotspot; individuals needing to perform sensitive transactions should use a personal VPN, such as the one shown in the accompanying figure.



count of unauthorized computer access, sentenced to two years in prison, and ordered to pay more than \$94,000 in restitution.

Develop Policies and Controls

All companies should develop policies and controls regarding security matters. As already mentioned, employees should be granted the least amount of access to the company network that they need to perform their job. Employees should be educated about the seriousness and consequences of hacking, data theft, and other computer crimes, and they should be taught what to do when they suspect a computer crime has been committed. Employees should also be instructed about proper computer and e-mail usage policies—such as whether or not downloading and installing software on company computers is allowed, whether or not employees are responsible for updating their computers, and the types of removable storage mediums (such as USB flash drives or portable digital media players) that may be used with company computers—in order to avoid inadvertently creating a security problem. Policies for removing computers and storage media containing sensitive data from the premises should also be implemented and enforced, and sensitive documents should be shredded when they are no longer needed. In addition, policies should be updated as needed to respond to new types of threats. For instance, the Pentagon banned USB flash drives in late 2008 due to a computer virus threat; it is unknown at this time when or if their use will be allowed again.

Employees who work from home or otherwise access the company network via the Internet also need to be educated about security policies for remote access and the proper precautions that need to be taken. These precautions include keeping their operating system and security software up to date, and using only encrypted storage devices (such as

self-encrypting USB flash drives) when transporting documents between work and home. In addition, telecommuting workers and outside contractors should not be allowed to have peer-to-peer (P2P) software on computers containing company documents, since data is increasingly being exposed through the use of P2P networks. For instance, classified data about the U.S. presidential helicopter was discovered recently on a computer in Iran and traced back to a P2P network and the computer of a military contractor in Maryland, and the Social Security numbers and other personal data belonging to about 17,000 current and former Pfizer workers were leaked onto a P2P network in 2007 after an employee installed unauthorized P2P software on a company notebook computer provided for use at her home.

Use Data-Leakage Prevention and Enterprise Rights-Management Software

As employees are increasingly bringing portable devices (such as mobile phones, portable digital media players, and USB flash drives) that can interact with business networks to the office, the challenge of securing these devices (and the company network against these devices) has grown. Some companies now prohibit all portable devices; others allow only company-issued devices so they can ensure appropriate security measures, such as encryption, password protection, and the ability to wipe the device clean remotely if it is lost or stolen, are implemented.

To protect against employees copying or sending confidential data to others either intentionally or accidentally, *data-leakage prevention systems* can be used. Data-leakage prevention systems are available as software and/or hardware systems, and have a range of capabilities, but the overall goal is to prevent sensitive data from exposure. For instance, some systems control which devices (such as USB flash drives and portable digital media players) can be connected to an employee's computer (see Figure 9-13) in order to prevent sensitive data from being taken home inadvertently or intentionally. Other data-leakage prevention systems—sometimes also called *outbound-content monitoring systems*—scan all outgoing communications (e-mail, transferred files, instant messages, and so forth) for documents containing Social Security numbers, intellectual property, and other confidential information. Some can also continually scan network devices to locate sensitive data in documents stored on computers to ensure that sensitive files are not on the computer of an employee who should not have access to them. For even stronger protection of confidential company documents, *enterprise rights-management software*, which encrypts confidential documents and limits functions such as printing, editing, and copying the data to only authorized users with the appropriate password, can be used.

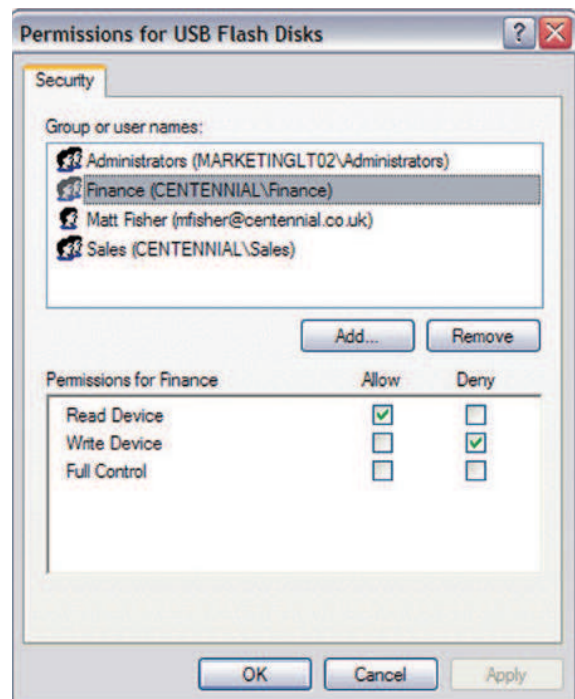


FIGURE 9-13
Data-leakage prevention software can control which devices can be connected to an employee's computer.

Ask Business Partners to Review their Security

In this networked economy, many organizations provide some access to internal resources for business partners. If those external companies are lax with their security measures, however, attacks through the business partners' computers (such as via an employee or hacker) are possible. Consequently, businesses should make sure that their business partners maintain adequate security policies and controls. Regulations—such as the *Sarbanes-Oxley Act of 2002*—increasingly require businesses to ensure that adequate controls are in place to preserve the integrity of financial reports. This includes outside companies—such as business partners and *outsourcing companies* (outside vendors for specific business tasks, as discussed in Chapter 12)—if they have access to sensitive corporate data. Companies that utilize cloud computing also need to ensure that the cloud vendor's policies (such as for protecting access to stored data, using adequate encryption techniques and backup procedures, submitting to necessary audits, and storing data in locations with the desired security and privacy laws) match the company's requirements.

COMPUTER SABOTAGE

Computer sabotage—acts of malicious destruction to a computer or computer resource—is another common type of computer crime today. Computer sabotage can take several forms, including launching a *computer virus* or a *denial of service (DoS) attack*, altering the content of a Web site, or changing data or programs located on a computer. A common tool used to perform computer sabotage is a *botnet*, discussed next. Computer sabotage is illegal in the United States, and acts of sabotage are estimated to cost individuals and organizations billions of dollars per year, primarily for labor costs related to correcting the problems caused by the sabotage, lost productivity, and lost sales.

Botnets

A computer that is controlled by a hacker or other computer criminal is referred to as a **bot** or *zombie computer*; a group of bots that are controlled by one individual and can work together in a coordinated fashion is called a **botnet**. According to the FBI, an estimated one million U.S. computers are currently part of a botnet; consequently, botnets are a major security threat. Criminals (called *botherders*) are increasingly creating botnets to use for computer sabotage, such as to spread *malware* and to launch *denial of service (DoS) attacks*, discussed shortly. Botherders also often sell their botnet services to send spam and launch Internet attacks on their clients' behalf, as well as use them to steal identity information, credit card numbers, passwords, corporate secrets, and other sensitive data, which are then sold to other criminals or otherwise used in an illegal manner.

Computer Viruses and Other Types of Malware

Malware is a generic term that refers to any type of malicious software. Malware programs are intentionally written to perform destructive acts, such as damaging programs, deleting files, erasing an entire hard drive, or slowing down the performance of a computer. This damage can take place immediately after a computer is *infected* (that is, the malware software is installed) or it can begin when a particular condition is met. A malware program that activates when it detects a certain condition, such as

when a particular keystroke is pressed or an employee's name is deleted from an employee file, is called a *logic bomb*. A logic bomb that is triggered by a particular date or time is called a *time bomb*.

Writing a computer virus or other type of malware or even posting the malware code on the Internet is not illegal, but it is considered highly unethical and irresponsible behavior. Distributing malware, on the other hand, is illegal, and virus writers who release their malware are being vigorously prosecuted. Malware can be very costly in terms of the labor costs associated with removing the viruses and correcting any resulting damage, as well as the cost of lost productivity of employees. One type of malware often used by computer criminals to send sensitive data secretly from

ASK THE EXPERT



Marian Merritt, Internet Safety Advocate, Symantec Corporation

How can individuals tell if their computers are part of a botnet?

Bots were created to steal your personal information or take control of your computer without you knowing. Because of that, they are silent in nature. The only way computer users can tell their computers are infected by a bot is by using a security solution with bot detection capabilities.

> **Computer sabotage.** An act of malicious destruction to a computer or computer resource. > **Bot.** A computer that is controlled by a hacker or other computer criminal. > **Botnet.** A group of bots that are controlled by one individual. > **Malware.** Any type of malicious software.

infected computers to the criminal—spyware—was discussed in Chapter 8. The most common other types of malware are discussed next.

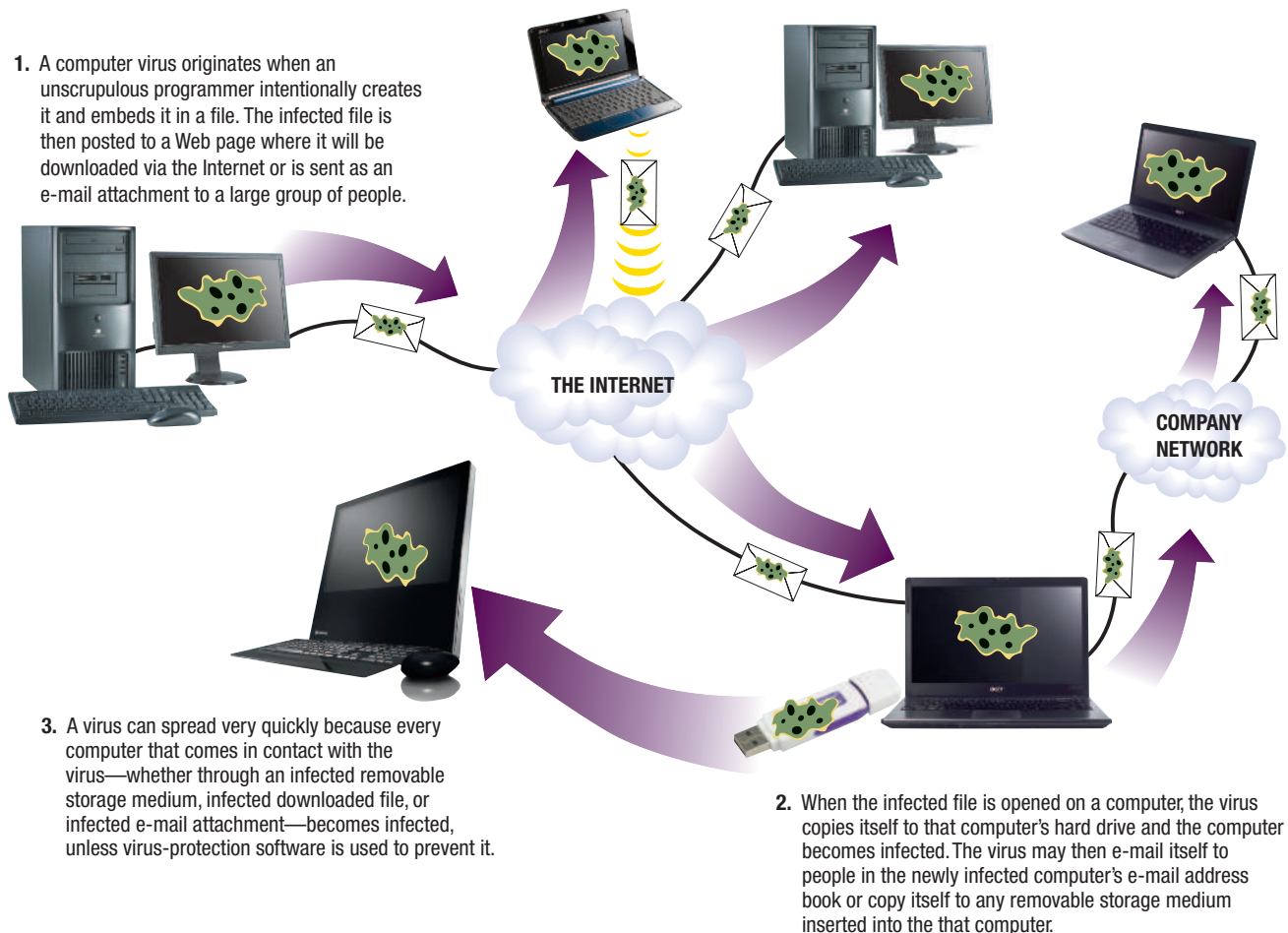
Computer Viruses

One type of malware is the **computer virus**—a software program that is installed without the permission or knowledge of the computer user, that is designed to alter the way a computer operates, and that can replicate itself to infect any new media it has access to. Computer viruses are often embedded into program or data files (often games, videos, and music files downloaded from Web pages or shared via a P2P service). They are spread whenever the infected file is downloaded, is transferred to a new computer via an infected removable storage medium, or is e-mailed to another computer (see Figure 9-14). Viruses can also be installed when a recipient clicks a link in an e-mail message (often in an unsolicited e-mail message that resembles a legitimate e-mail message that normally contains a link, such as an electronic greeting card e-mail that contains a link to view the card), as well as through links in instant messages. Regardless of how it is obtained, once a copy of the infected file reaches a new computer it typically embeds itself into program, data, or system files on the new computer and remains there, affecting that computer according to its programmed instructions, until it is discovered and removed.

TIP

It is common practice for all types of malware to be referred to generically as “viruses,” even though some may not technically be computer viruses.

FIGURE 9-14
How a computer virus or other type of malicious software might spread.



>Computer virus. A software program installed without the user's knowledge and designed to alter the way a computer operates or to cause harm to the computer system.



ONLINE VIDEO

Go to the Chapter 9 page at www.cengage.com/computerconcepts/np/uc13 to watch the "How Worms Spread Using AutoPlay" video clip.

Computer Worms

Another common form of malware is the **computer worm**. Like a computer virus, a computer worm is a malicious program that is typically designed to cause damage. Unlike a computer virus, however, a computer worm does not infect other computer files on the infected computer in order to replicate itself; instead, it spreads by creating copies of its code and sending those copies to other computers via a network. Often, the worm is sent to other computers as an e-mail attachment. Usually after the infected e-mail attachment is opened by an individual, the worm inflicts its damage and then automatically sends copies of itself to other computers via the Internet or a private network, typically using addresses in the e-mail address book located on the newly infected computer. When those e-mail messages and their attachments are opened, the new computers become infected and the cycle continues. Because of its distribution method, a worm can spread very rapidly. For instance, the *Mydoom* worm (which was released in 2004 and is considered one of the fastest spreading worms ever) spread so rapidly that, at one point, one out of every 10 e-mails contained the worm.

Some newer worms do not require any action by the users (such as opening an e-mail attachment) to infect their computers. Instead, the worm scans the Internet looking for computers that are vulnerable to that particular worm and sends a copy of itself to those computers to infect them. Other worms just require the user to view an infected e-mail message or insert an infected removable storage medium (such as a USB flash drive) into the computer, in order to infect the computer. Still other worms are specifically written to take advantage of newly discovered *security holes* (vulnerabilities) in operating systems and e-mail programs. Worms and other types of malware that are designed to take advantage of a security hole and are released at a time when no security patch to correct the problem is available are referred to as *zero-day attacks*. Unfortunately, as malware writing tools become more sophisticated, zero-day attacks are becoming more common.

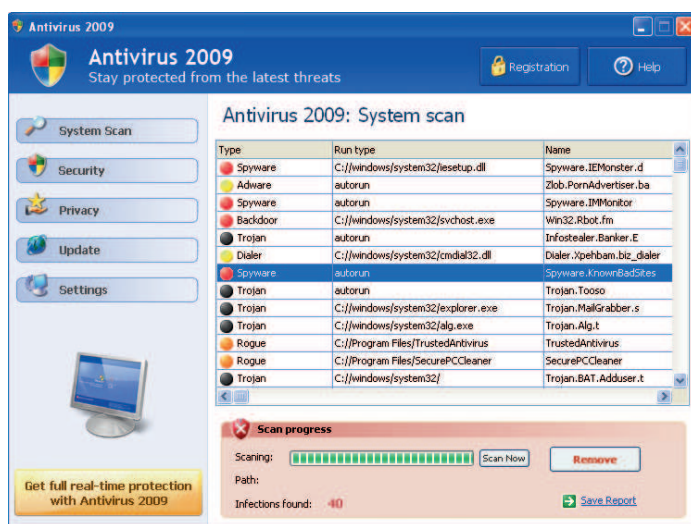


FIGURE 9-15

Rogue antivirus programs. These programs try to trick victims into purchasing subscriptions to remove nonexistent malware supposedly installed on their computers.

Trojan Horses

A **Trojan horse** is a type of malware that masquerades as something else—usually an application program (such as what appears to be a game or utility program). When the seemingly legitimate program is downloaded or installed, the malware part of the Trojan horse infects the computer. Many recent Trojan horses masquerade as normal ongoing activities (such as the Windows Update service or an *antivirus* or *antispyware* program telling you to download a file containing program updates) when they are installed to try to trick unsuspecting users into downloading another malware program or buying a useless program. For instance, after a *rogue antivirus* program like the one shown in Figure 9-15 is installed (usually without the user's direct knowledge or permission), the malware takes over the computer displaying warning messages or scan results (see Figure 9-15) indicating the computer is infected with malware. In addition, the rogue antivirus program typically prevents access to any Web sites other than its own and prompts the user to buy a fake anti-malware program to get rid of the "malware." Usually the only malware on the computer is the rogue program,



- > **Computer worm.** A malicious program designed to spread rapidly to a large number of computers by sending copies of itself to other computers.
- > **Trojan horse.** A malicious program that masquerades as something else.

but it is often very intrusive (such as displaying constant messages on the desktop and in pop-up windows and hiding the options needed to change the hijacked settings back to normal), and it is extremely hard to remove.

Unlike viruses and worms, Trojan horses cannot replicate themselves. Trojan horses are usually spread by being downloaded from the Internet, though they may also be sent as an e-mail attachment, either from the Trojan horse author or from individuals who forward it, not realizing the program is a Trojan horse. Some Trojan horses today act as spyware and are designed to find sensitive information about an individual (such as a Social Security number or a bank account number) or about a company (such as corporate intellectual property like mechanical designs, electronic schematics, and other valuable proprietary information) located on infected computers and then send that information to the malware creator to be used in illegal activities. One emerging type of Trojan horse is called a *RAT* (*Remote-Access Trojan*). RATs are typically installed via small files obtained from an Internet download, such as free software, games, or electronic greeting cards. Once installed, RATs are designed to record every keystroke made on the infected computer and then send the sensitive information they recorded (such as account numbers and passwords) to criminals.

Mobile Malware

In addition to computers, malware also can infect mobile phones, portable digital media players, printers, and other devices that contain computing hardware and software. In fact, some GPS devices and portable digital media players (including some video iPods) shipped recently had malware already installed on them. Mobile phones with Bluetooth capabilities in particular are vulnerable since they can be infected via a Bluetooth connection just by being within range (about 30 feet) of a carrier. Some *mobile malware* is designed to crash the phone's operating system; others are designed to be a nuisance by changing icons or otherwise making the device more difficult to use. Still others are money-oriented, such as malware designed to steal credit card data located on the mobile phone. According to IBM, more malware directed to mobile phones and other devices—such as cars—that contain embedded computers is expected in the near future as those devices continue to incorporate more software components and, consequently, become more vulnerable to malware. However, the lack of a universal operating system for mobile devices (compared with the relatively few operating systems used with personal computers) at the present time limits the amount of mobile malware currently in circulation.

Denial of Service (DoS) Attacks

A **denial of service (DoS) attack** is an act of sabotage that attempts to flood a network server or Web server with so many requests for action that it shuts down or simply cannot handle legitimate requests any longer, causing legitimate users to be denied service. For example, a hacker might set up one or more computers to *ping* (contact) a server continually with a request to send a responding ping back to a false return address, or to request nonexistent information continually. If enough useless traffic is generated, the server has no resources left to deal with legitimate requests (see Figure 9-16). An emerging trend is DoS attacks aimed at mobile wireless networks. These attacks typically involve repeatedly establishing and releasing connections with the goal of overloading the network to disrupt service.

> **Denial of service (DoS) attack.** An act of sabotage that attempts to flood a network server or a Web server with so much activity that it is unable to function.

ONLINE VIDEO



Go to the Chapter 9 page at

[www.cengage.com/](http://www.cengage.com/computerconcepts/np/uc13)

[computerconcepts/np/uc13](http://www.cengage.com/computerconcepts/np/uc13)

to watch the "Demonstration of a Rogue Antivirus Program Spread via Skype" video clip.

FURTHER EXPLORATION

Go

Go to the Chapter 9 page at

[www.cengage.com/](http://www.cengage.com/computerconcepts/np/uc13)

[computerconcepts/np/uc13](http://www.cengage.com/computerconcepts/np/uc13)

for links to information about malware and malware detection.

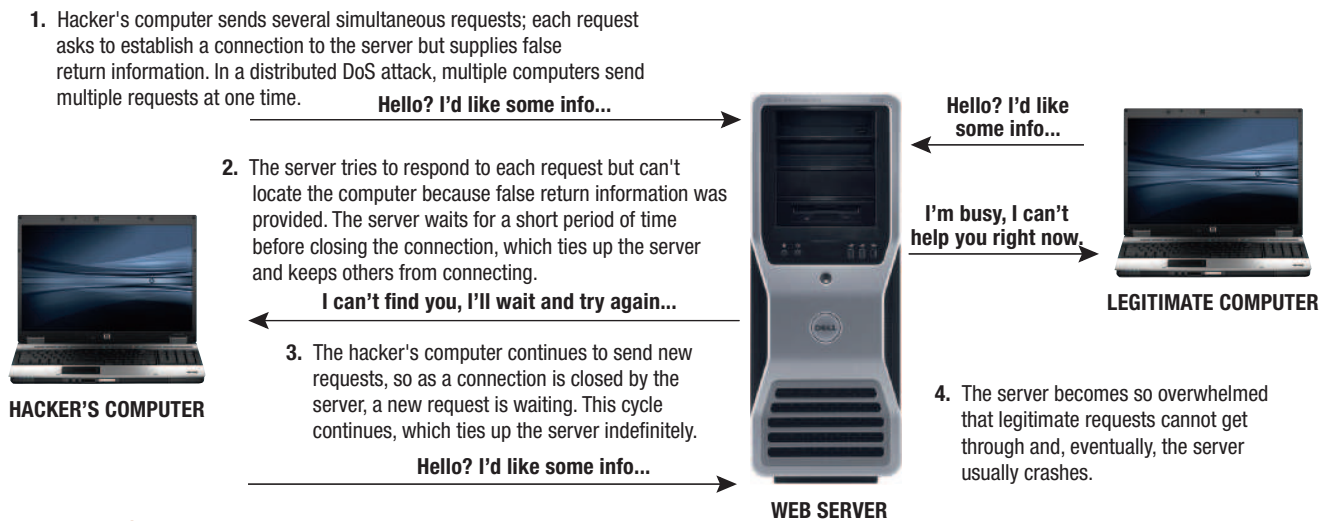


FIGURE 9-16
How a denial of service (DoS) attack might work.

DoS attacks today are often directed toward popular sites (for example, Twitter was recently shut down for two hours due to a DoS attack) and typically are carried out via multiple computers (referred to as a *distributed denial of service attack* or *DDoS attack*). DDoS attacks are typically performed by botnets created by hackers; the computers in the botnet participate in the attacks without the owners' knowledge. Because home computers are increasingly using direct Internet connections but tend to be less protected than school and business computers, hackers are increasingly targeting home computers for botnets used in DDoS attacks and other forms of computer sabotage.

Denial of service attacks can be very costly in terms of business lost (such as when an e-commerce site is shut down), as well as the time and expense required to bring the site back online. Networks that use VoIP are particularly vulnerable to DoS attacks since the real-time nature of VoIP calls means their quality is immediately affected when a DoS attack slows down the network.

Data, Program, or Web Site Alteration

Another type of computer sabotage occurs when a hacker breaches a computer system in order to delete data, change data, modify programs, or otherwise alter the data and programs located there. For example, a student might try to hack into the school database to change his or her grade; a hacker might change a program located on a company server in order to steal money or information; or a disgruntled or former employee might perform a vengeful act, such as altering programs so they work incorrectly, deleting customer records or other critical data, or randomly changing data in a company's database. Like other forms of computer sabotage, data and program alteration is illegal.

Data on Web sites can also be altered by hackers. For instance, individuals sometimes hack into and alter other people's social networking accounts. In early 2009, for instance, the Twitter accounts of over 30 high-profile individuals (including then President-elect Obama) were accessed by an unauthorized individual who sent out fake (and sometimes embarrassing) tweets posing as those individuals. It is also becoming more common for hackers to compromise legitimate Web sites and then use those sites to perform malware attacks. Typically, a hacker alters a legitimate site to display an official-looking message that informs the user that a particular software program must be downloaded, or the hacker posts a rogue banner ad on a legitimate site that redirects the user to a malware site instead of the site for the product featured in the banner ad. According to a report released this year by security company Websense, more than half of the Web sites classified as malicious are actually legitimate Web sites that have been compromised.

PROTECTING AGAINST COMPUTER SABOTAGE

One of the most important protections against computer sabotage is using *security software*, and ensuring that it is kept current.

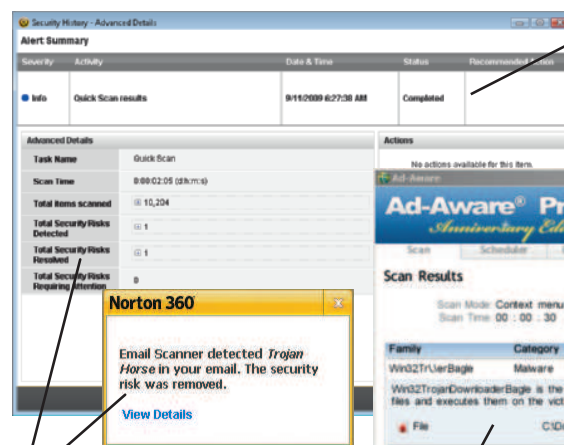
Security Software

To protect against becoming infected with a computer virus or other type of malware, all computers and other devices used to access the Internet or a company network in both homes and offices should have **security software** installed. Security software typically includes a variety of security features, including a firewall, protection against spyware and bots, and protection against some types of *online fraud*, discussed shortly. One of the most important components is **antivirus software**, which protects against computer viruses and other types of malware.

Antivirus software typically runs continuously whenever the computer is on to perform real-time monitoring of the computer and incoming e-mail messages, instant messages, Web page content, and downloaded files, in order to prevent malicious software from executing. Many antivirus programs also automatically scan any devices as soon as they are connected to a USB port in order to guard against infections from a USB flash drive, a portable digital media player, or other USB device. Antivirus software helps prevent malware from being installed on your computer since it deletes or *quarantines* (safely isolates) any suspicious content (such as e-mail attachments or downloaded files) as they arrive; regular full system scans can detect and remove any viruses or worms that find their way onto your computer (see Figure 9-17).

According to McAfee Security, a manufacturer of antivirus and security software, there are millions of threats in existence today, and research firm IDC estimates that 450 new viruses and other types of malware are released each day. Consequently, it is vital to keep your antivirus program up to date. Antivirus software is usually set up to download new *virus definitions* automatically from its associated Web site on a regular basis, as often as several times per day—a very important precaution. Most fee-based antivirus programs come with a year of access to free updates; users should purchase additional years after that to continue to be protected or they should switch to a free antivirus program, such as *AVG Free*, that can be updated regularly at no cost. Schools and businesses should also ensure

ANTIVIRUS SOFTWARE



If malware is found during a scan or as you use your computer, the software removes it.

TIP

To ensure you have the latest security updates for your antivirus program, enable *automatic updates*.

VIDEO PODCAST

Go to the Chapter 9 page at www.cengage.com/computerconcepts/np/uc13 to download or listen to the “How To: Protect Yourself Against Malware” video podcast.

FIGURE 9-17
Security software.

Most security software is set up to monitor your system on a continual basis, removing threats as they are discovered.

Both programs typically monitor your system on a continual basis, as well as periodically scanning your entire computer.



If spyware is found, the software recommends quarantining or removing it.

ANTISPYWARE SOFTWARE

>**Security software.** Software, typically a suite of programs, used to protect your computer against a variety of threats. >**Antivirus software.** Software used to detect and eliminate computer viruses and other types of malware.

VIRUS PREVENTION STRATEGIES

Use antivirus software to check incoming e-mail messages and files, and download updated virus definitions on a regular basis.

Limit the sharing of flash memory cards, USB flash drives, and other removable storage media with others.

Only download files from reputable sites.

Only open e-mail attachments that come from people you know and that do not have an executable file extension (such as .exe, .com, .bat, or .vbs); double-check with the sender before opening an unexpected, but seemingly legitimate, attachment.

For any downloaded file you are unsure of, upload it to a Web site (such as VirusTotal.com) that tests files for viruses before you open them.

Keep the preview window of your e-mail program closed so you will not view messages until you determine that they are safe to view.

Regularly download and install the latest security patches available for your operating system, browser, and e-mail programs.

Avoid downloading files from P2P sites.



FIGURE 9-18

Sensible precautions can help protect against computer virus infections.

TIP

If you suspect you are infected with a malware program that your antivirus software cannot detect or remove, try a software program that specializes in removing hard-to-remove malware, such as the free *MalwareBytes Anti-Malware* program.

that students and employees connecting to the campus or company network with personal computers are using up-to-date antivirus software so they will not infect the network with malware inadvertently. Some colleges now require new students to go through a *quarantine process*, in which students are not granted access to the college network until they complete a security process that checks their computers for security threats, updates their operating systems, and installs antivirus software. Some additional virus-prevention strategies are listed in Figure 9-18.

Many ISPs today also offer some malware protection to their subscribers. Typically, ISP antivirus software scans all incoming e-mail messages at the mail server level to filter out messages containing a virus. If a message containing a virus is detected, it is usually deleted and the recipient is notified that the message contained a virus and was deleted. Another type of program, which is currently in development and which is designed to protect against viruses sent via e-mail, is an *e-mail authentication system*. E-mail

authentication systems are designed to tell recipients exactly where e-mail messages come from to help them determine which messages are safe to open and which might contain malware. For a look at an emerging tool in the fight against malware—*people-driven security* and *whitelisting*—see the Inside the Industry box.

Other Security Precautions

Individuals and businesses can protect against some types of computer sabotage (such as program, data, or Web site alteration) by controlling access to their computers and networks, as discussed earlier in this chapter. Intrusion protection systems can help businesses detect and protect against denial of service (DoS) attacks. For extra protection against spyware, rogue antivirus programs, and other specialized malware, specialized security programs (such as the antispyware program shown in Figure 9-17 for detecting and removing spyware) can be used. In addition, most Web browsers have security settings that can be used to help prevent programs from being installed on a computer without the user's permission, such as prompting the user for permission whenever a download is initiated. Enabling these security settings is a wise additional precaution.

ONLINE THEFT, ONLINE FRAUD, AND OTHER DOT CONS

A booming area of computer crime involves online fraud, theft, scams, and related activities designed to steal money or other resources from individuals or businesses—these are collectively referred to as **dot cons**. According to a report by the *Internet Crime Complaint Center (IC3)*, a joint venture of the FBI and the National White Collar Crime Center that receives cybercrime complaints from consumers and reports them to the appropriate law enforcement agency, online crime hit a record high in 2008. In all, more than

➤ **Dot con.** A fraud or scam carried out through the Internet.

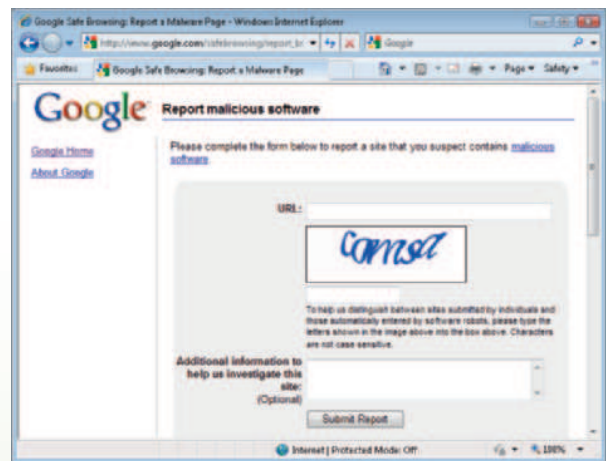
INSIDE THE INDUSTRY

New Tools to Fight Malware

People-driven security refers to using the judgments of individuals to identify new threats. For instance, Google has a page where users can submit URLs of Web sites they believe are malicious (see the accompanying illustration), and antivirus companies like Symantec and McAfee rely on malware samples that they receive from users to help keep their virus lists and programs current. Many security experts believe that user involvement is crucial today in the fight against malware and phishing. People-driven security is also being used today to identify spammers.

The idea behind *whitelisting* is the opposite of blocking potentially dangerous applications from running on your computer; with whitelisting, only known good programs are allowed to run. While some users believe that whitelisting is annoying (because trying to run a program not on the whitelist requires responding to a pop-up alert message), many security companies believe that keeping track of known good software might be easier than trying to keep track of all the malware in existence today. Both Symantec and Kaspersky Lab are advocates of whitelisting and Kaspersky recently integrated the database

of Bit9, a company that maintains a list of over six billion known good applications, into its antivirus programs. While antivirus companies are currently working on maintaining their own whitelists to use in conjunction with their products, some view a central whitelist maintained by a neutral group and available to everyone as the most efficient solution for consumers.



275,000 reports were received with an average individual loss of \$931. Some of the most common types of dot cons are discussed next.

Theft of Data, Information, and Other Resources

Data theft or *information theft* is the theft of data or information located on or being sent from a computer. It can be committed by stealing an actual computer (as discussed in more detail in Chapter 15); it can also take place over the Internet or a network by an individual gaining unauthorized access to that data by hacking into the computer or by intercepting the data in transit. Common types of data and information stolen via the Internet or another network include customer data (such as Web site passwords or credit card information) and proprietary corporate information. Over the past years, there have been numerous examples of hackers stealing information from company databases. For instance, one hacker obtained the contact information of more than 1.6 million users of the Monster.com online job search service; another breached the systems of the Heartland credit and debit card processor and several retail stores, stealing more than 130 million credit and debit card numbers, according to the charges filed against the hacker. Stolen consumer data is often used in fraudulent activities, such as *identity theft*, as discussed shortly.

Money is another resource that can be stolen via a computer. Company insiders sometimes steal money by altering company programs to transfer small amounts of money—for example, a few cents' worth of bank account interest—from a very large number of transactions to an account controlled by the thieves. This type of crime is sometimes called *salami shaving*. Victims of salami-shaving schemes generally are unaware that their funds have been accessed because the amount taken from each individual is very small. However, added together, the amounts can be substantial. Another example of monetary theft performed via computers involves hackers electronically transferring money illegally from

online bank accounts, traditional bank accounts, credit card accounts, or accounts at online payment services (such as *PayPal*, which is discussed more in Chapter 11).

Identity Theft, Phishing, and Pharming

A growing dot con trend is obtaining enough information about an individual to perform fraudulent financial transactions. Often, this is carried out in conjunction with *identity theft*; techniques frequently used to obtain the necessary personal information to commit identity theft are *phishing*, *spear phishing*, and *pharming*. These topics are discussed next.

TIP

To help prevent identity theft, do not include your Social Security number on your résumé or any other document posted online.

Identity Theft

Identity theft occurs when someone obtains enough information about a person to be able to masquerade as that person—usually to buy products or services in that person’s name (see Figure 9-19). Typically, identity theft begins with obtaining a person’s name, address, and Social Security number, often from a discarded or stolen document (such as a preapproved credit card application that was sent in the mail), from information obtained via the Internet (such as from a résumé posted online), or from information located on a computer (such as on a stolen computer or hacked server, or information sent from a computer via a computer virus or spyware program installed on that computer). The thief may then order a copy of the individual’s birth certificate, obtain a “replacement” driver’s license, make purchases and charge them to the victim, and/or open credit or bank accounts in the victim’s name. Identity theft is illegal and, in 1998, the federal government passed the *Identity Theft and Assumption Deterrence Act*, which made identity theft a federal crime.

Assuming the thief requests a change of address for these new accounts after they are opened, it may take quite some time—often until a company or collections agency contacts the victim about overdue bills—for the victim to become aware that his or her identity has been stolen. Although identity theft often takes place via a computer today, information used in identity theft can also be gathered from trash dumpsters, mailboxes, and other locations. Other commonly used techniques are *skimming* and *social engineering*. Skimming involves stealing credit card or debit card numbers by using an illegal device attached to an ATM machine or credit card reader that reads and stores the card numbers to be retrieved by the thief

FIGURE 9-19
How identity theft works.



1. The thief obtains information about an individual from discarded mail, employee records, credit card transactions, Web server files, or some other method.
2. The thief uses the information to make purchases, open new credit card accounts, and more in the victim's name. Often, the thief changes the address on the account to delay the victim's discovery of the theft.
3. The victim usually finds out by being denied credit or by being contacted about overdue bills generated by the thief. Clearing one's name after identity theft is time-consuming and can be very difficult and frustrating for the victim.

> **Identity theft.** Using someone else's identity to purchase goods or services, obtain new credit cards or bank loans, or otherwise illegally masquerade as that individual.

at a later time. Social engineering involves pretending—typically via phone or e-mail—to be a bank officer, potential employer, or other trusted individual in order to get the potential victim to supply personal information. One recent social engineering scheme placed phony parking tickets on cars instructing the owners to go to a particular Web site; going to that site installed software on the users' computers to capture their keystrokes.

Unfortunately, identity theft is a very real danger to individuals today. According to the Federal Trade Commission (FTC), millions of Americans have their identity stolen each year. Identity theft can be extremely distressing for victims, can take years to straighten out, and can be very expensive. Some identity theft victims, such as Michelle Brown, believe that they will always be dealing with their “alter reality” to some extent. For a year and a half, an identity thief used Brown's identity to obtain over \$50,000 in goods and services, to rent properties—even to engage in drug trafficking. Although the culprit was eventually arrested and convicted for other criminal acts, she continued to use Brown's identity and was even booked into jail using Brown's stolen identity. As a final insult after the culprit was in prison, U.S. customs agents detained the real Michelle Brown when she was returning from a trip to Mexico because of the criminal record of the identity thief. Brown states that she has not traveled out of the country since, fearing an arrest or some other serious problem resulting from the theft of her identity, and estimates she has spent over 500 hours trying to correct all the problems related to the identity theft.

Phishing and Spear Phishing

Phishing (pronounced “fishing”) is the use of a *spoofed* e-mail message (an e-mail appearing to come from eBay, PayPal, Bank of America, or another well-known legitimate organization, but is actually sent from a phisher) to trick the recipient into revealing sensitive personal information (such as Web site logon information or credit card numbers). Once obtained, this information is used in identity theft and other fraudulent activities. A phishing e-mail typically looks legitimate and it contains links in the e-mail that appear to go to the Web site of the legitimate business, but these links go to the phisher's Web site that is set up to look like the legitimate site instead—an act called *Web site spoofing*. Phishing e-mails are typically sent to a wide group of individuals and usually include an urgent message stating that the individual's credit card or account information needs to be updated and instructing the recipient of the e-mail to click the link provided in the e-mail in order

ASK THE EXPERT



Marian Merritt, Internet Safety Advocate, Symantec Corporation

What is the single most important thing computer users should do to protect themselves from online threats?

The single most important step to protect computer users from online threats is to make sure their Internet security solution is current and up to date. There are several all-in-one security solutions available, such as Symantec's Norton 360, which combine PC security, antiphishing capabilities, backup, and tuneup technologies.

It's also pivotal to maintain a healthy wariness when receiving online communications. Do not click on links in suspicious e-mails or instant messages (IMs). These links will often direct you to sites that will ask you to reveal passwords, PINs, or other confidential data. Genuine organizations or institutions do not send such e-mails, nor do they ask for confidential data (like your Social Security number) for ordinary business transactions. If you're unsure whether or not an e-mail is legitimate, type the URL directly in your browser or call the institution to confirm they sent you that e-mail. Finally, do not open attachments in e-mails of questionable origin, since they may contain viruses.

> **Phishing.** The use of spoofed e-mail messages to gain credit card numbers and other personal data to be used for fraudulent purposes.

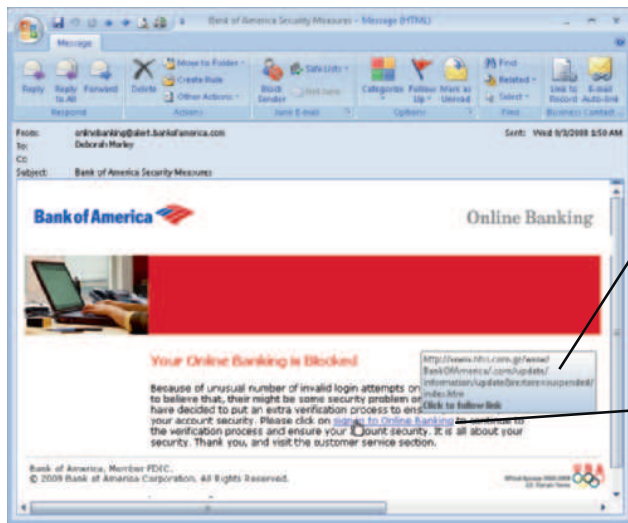


FIGURE 9-20

Phishing. Phishing schemes use legitimate-looking e-mails to trick users into providing private information.

to keep the account active (see Figure 9-20). If the victim clicks the link and supplies the requested information via the spoofed site, the criminal gains access to all information provided by the victim, such as account numbers, credit card numbers, and Web site passwords. Phishing attempts can occur today via IM, text messages (called *smishing*), fake messages sent via eBay or MySpace, Twitter tweets, and pop-up security alert windows, in addition to via e-mail. Phishers also frequently utilize spyware; typically, clicking the link in the phishing e-mail installs the spyware on the victim's computer, and it will remain there (transmitting passwords and other sensitive data to a phisher) until it is detected and removed.

To fool victims into using the spoofed Web site, phishing e-mails and the spoofed Web sites

often look legitimate. To accomplish this, phishers typically use copies of the spoofed organization's logo and other Web site content from the legitimate Web site. For spoofed banking Web pages and other pages where the victim would expect to see a secure Web page, some criminals use a secure connection between the victim and the criminal's server so the Web page looks secure with an *https:* in the Address bar. The domain name of the legitimate company (such as *ebay* for an eBay phishing page) is also often used as part of the URL of the phishing link (such as a URL starting with the text *ebay* even though the URL's domain is not *ebay.com*) to make it appear more legitimate. Other phishing schemes use a technique called *typosquatting*, which is setting up spoofed Web sites with addresses slightly different from legitimate sites. For example, a spoofed Web site using the URL *www.amazom.com* might be used to catch shoppers intending to reach the Amazon.com Web site located at *www.amazon.com* in hopes that customers making this error when typing the URL will not notice it and will supply logon information via the spoofed site when they arrive at it.

Another recent trend is the use of more targeted, personalized phishing schemes, known as **spear phishing**. Spear phishing e-mails are directly targeted to a specific individual and typically appear to come from an organization or person that the targeted individual has an association with. They also often include personalized information (such as the potential victim's name) to make the spear phishing e-mails seem even more legitimate. Several recent spear phishing attacks were targeted at users of social networking sites like MySpace since the personal information (name, age, hobbies, friends list, favorite music, and so forth) typically included on these sites makes them a good resource for spear phishers. Some of these attacks used spoofed logon pages for the social networking sites to obtain an individual's logon information and password. Since many individuals use the same logon information for a variety of sites, once a scammer has a valid username/password combination, he or she can try it on a variety of common e-commerce sites, such as shopping sites, online banking sites, and online payment services like PayPal. If the scammer is able to log on successfully to one of these sites, he or she can buy products, transfer money, and perform other types of financial transactions posing as the victim. Another recent tactic is to use the victim's social networking site logon information to log on to the victim's account and then post comments or send messages containing phishing links (posing as the victim) to the victim's friends, who are much more likely to click on the links because they appear to come from a friend.

➤ **Spear phishing.** A personalized phishing scheme targeted at an individual.

Spear phishers also target employees of selected organizations by posing as someone within the company, such as a human resources or technical support employee. These spear phishing e-mails often request confidential information (such as logon IDs and passwords) or direct the employee to click a link to supposedly reset his or her password. The goal for corporate spear phishing attacks is usually to steal intellectual property, such as software source code, design documents, or schematics. It can also be used to steal money. For instance, in one recent case, a grocery store received fraudulent e-mails that appeared to come from two approved suppliers. The e-mails instructed the grocery store chain to send future payments to new bank accounts listed in the e-mail—the grocery store chain deposited more than \$10 million into two fraudulent bank accounts before the scam was discovered.

Pharming and Drive-By Pharming

Pharming is another type of scam that uses spoofing—specifically spoofed domain names used to obtain personal information for use in fraudulent activities. With pharming, the criminal reroutes traffic intended for a commonly used Web site to a spoofed Web site set up by the pharmer. Sometimes pharming takes place via malicious code sent to a computer via an e-mail message or other distribution method. More often however, it takes place via changes made to a *DNS server*—a computer that translates URLs into the appropriate IP addresses needed to display the Web page corresponding to a URL. This type of pharming can take place at one of the 13 *root DNS servers* (the DNS servers used in conjunction with the Internet), but it more often takes place at a *company DNS server* (the DNS server for that company used to route Web page requests received via company Web site URLs to the appropriate company server). After hacking into a company DNS server (typically for a company with a commonly used Web site), the pharmer changes the IP addresses used in conjunction with a particular company URL (called *DNS poisoning*) so any Web page requests made via the legitimate company URL is routed (via the company's poisoned DNS server) to a phony spoofed Web page located on the pharmer's Web server. So, even though a user types the proper URL to display the legitimate company Web page in his or her browser, the spoofed page is displayed instead.

Since spoofed sites are set up to look like the legitimate sites, the user typically does not notice any difference, and any information sent via that site is captured by the pharmer. To avoid suspicion, some pharming schemes capture the user's account name and password as it is entered the first time on the spoofed site, and then display a password error message. The spoofed site then redirects the user back to the legitimate site where he or she is able to log on to the legitimate site, leaving the user to think that he or she must have just mistyped the password the first time. But, by then, the pharmer has already captured the victim's username and password and can use that information to gain access to the victim's account.

A recent variation of pharming is *drive-by pharming*. The goal is still to redirect victims to spoofed sites; however, the pharmer accomplishes this by changing the victim's designated DNS server (which is specified in the victim's router settings) to the pharmer's DNS server in order to direct the victim to spoofed versions of legitimate Web sites when the victim enters the URLs for those sites. Typically, the pharmer uses malicious JavaScript code placed on a Web page to changes the victim's DNS settings to use the pharmer's DNS server; this change can only occur on a router in which the default administrator password was not changed.

Online Auction Fraud

Online auction fraud (sometimes called *Internet auction fraud*) occurs when an online auction buyer pays for merchandise that is never delivered, or that is delivered but it is

➤ **Pharming.** The use of spoofed domain names to obtain personal information to be used in fraudulent activities. ➤ **Online auction fraud.** When an item purchased through an online auction is never delivered after payment, or the item is not as specified by the seller.

not as represented. Online auction fraud is an increasing risk for online auction bidders. According to the Internet Crime Complaint Center (IC3), online auction fraud accounted for about 25% of all reported online fraud cases in 2008 for an average loss of around \$600. Like other types of fraud, online auction fraud is illegal, but similar to many types of Internet cons, prosecution is difficult for online auction fraud because multiple jurisdictions are usually involved. Although most online auction sites have policies that suspend sellers with a certain number of complaints lodged against them, it is very easy for those sellers to come back using a new e-mail address and identity.

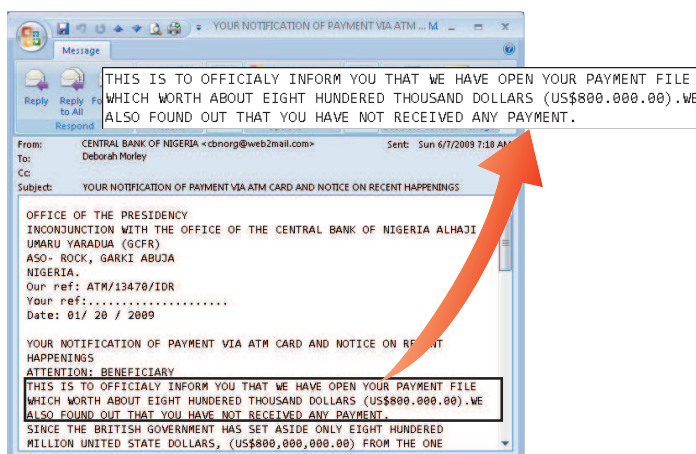
Other Internet Scams

There is a wide range of other scams that can occur via Web sites or unsolicited e-mails. The anonymity of the Internet makes it very easy for con artists to appear to be almost anyone they want to be, including a charitable organization or a reputable-looking business. Common types of scams include loan scams, work-at-home cons, pyramid schemes, bogus credit card offers and prize promotions, and fraudulent business opportunities and franchises. These offers typically try to sell potential victims nonexistent services or worthless information, or they try to convince potential victims to voluntarily supply their credit card details and other personal information, which are then used for fraudulent purposes. Some scammers use hacking as a means of obtaining a list of e-mail addresses for potential targets for a scam (such as stealing contact information from sites related to investing for a stock market scam) to increase the odds of a potential victim falling for the scam. A recent trend involves scammers who hack into Web mail and social networking accounts and send messages (posing as the victim) to the victim's entire contact list requesting money or urging recipients to buy specific products.

One ongoing Internet scam is the *Nigerian letter fraud* scheme. This scheme involves an e-mail message that appears to come from the Nigerian government and that promises the potential victim a share of a substantial amount of money in exchange for the use of the victim's bank account. Supposedly the victim's bank account information is needed to facilitate a wire transfer (but the victim's account is emptied instead) and/or up-front cash is needed to pay for nonexistent fees (that is kept by the con artist with nothing given in return). The theme of these scams often changes to fit current events, such as the war in Iraq or the Katrina hurricane. However, the scams always involve a so-called fortune that is inaccessible to the con artist without the potential victims' help (see Figure 9-21) and the victims always lose money when they pay fees or provide bank account information in the hope of sharing in the wealth. Despite the fact that this con is well known, people are still falling for it and with heavy losses—at \$1,650, the Nigerian letter fraud scam had the third highest average dollar loss per individual for 2008 complaints, according to a report issued by the Internet Crime Complaint Center (IC3).

Other schemes involve con artists who solicit donations after disasters and other tragic events, but who keep the donations instead of giving them to any charitable organization. Another common scam involves setting up a pornographic site that requires a valid credit card, supposedly to prove that the visitor is of the required age (such as over 18), but which is then used for credit card fraud. A relatively new type of scam involves posting fake job listings on job search sites to elicit personal information (such as Social Security numbers) from job seekers. An even more recent twist is to hire individuals through online job sites for seemingly legitimate positions involving money handling (such as bookkeeping or accounting positions), but then use those individuals—often without their knowledge—as illegitimate go-betweens to facilitate Internet auction scams and other monetary scams.

FIGURE 9-21
A Nigerian letter
fraud e-mail.



PROTECTING AGAINST ONLINE THEFT, ONLINE FRAUD, AND OTHER DOT CONS

In a nutshell, the best protection against many dot cons is protecting your identity; that is, protecting any identifying information about you that could be used in fraudulent activities. There are also specific precautions that can help protect against online theft, identity theft, online auction fraud, and other types of dot cons, as discussed next. With any dot con, it is important to act quickly if you think you have been a victim. For instance, you should work with your local law enforcement agency, credit card companies, and the three major consumer credit bureaus (*Equifax*, *Experian*, and *TransUnion*) to close any accessed or fraudulent accounts, place fraud alerts on your credit report, and take other actions to prevent additional fraudulent activity while the fraud is being investigated.

Arrests and prosecutions by law enforcement agencies may also help cut down on cybercrimes. Prosecution of online scammers has been increasing and sentences are not light. For instance, one man—the first person convicted by a jury under the *CAN-SPAM Act of 2003* for operating a phishing scheme—was sentenced in mid-2007 to 70 months in federal prison and ordered to pay over one million dollars to his victims.


Protecting Against Data and Information Theft

Businesses and individuals can both help to prevent some types of data and information theft. For instance, businesses should use good security measures to protect the data stored on their computers. Individuals should be vigilant about protecting their private information by sending sensitive information via secure Web servers only and not disclosing personal information—especially a Social Security number or a mother's maiden name—unless it is absolutely necessary and they know how the information will be used and that it will not be shared with others. In addition, individuals should never give out sensitive personal information to anyone who requests it over the phone or by e-mail—businesses that legitimately need bank account information, passwords, or credit card numbers will not request that information via phone or e-mail. Encrypting computers and other hardware containing sensitive information, so it will not be readable if the hardware is lost or stolen, is another important precaution.

Protecting Against Identity Theft, Phishing, and Pharming

Some of the precautions used for other types of online theft (such as being careful to disclose your personal information only when it is necessary and only via secure Web pages) can help reduce the chance that identity theft will happen to you. So can using security software (and keeping it up to date) to guard against computer viruses, spyware, and other malware that can be used to send information from your computer or about your activities (the Web site passwords that you type, for example) to a criminal. In addition, to prevent someone from using the preapproved credit card offers and other documents containing personal information that frequently arrive in the mail, shred them before throwing them in the trash. To prevent the theft of outgoing mail containing sensitive information, don't place it in your mailbox—mail it at the post office or in a USPS drop box.

To avoid phishing schemes, never click a link in an e-mail message to go to a secure Web site—always type the URL for that site in your browser (not necessarily the URL shown in the e-mail message) instead. Phishing e-mails typically sound urgent and often contain spelling and grammatical errors—see Figure 9-22 for some tips to help you recognize phishing e-mails. Remember that

 **FIGURE 9-22**
Tips for identifying
phishing e-mail
messages.

A PHISHING E-MAIL OFTEN . . .

Tries to scare you into responding by sounding urgent, including a warning that your account will be cancelled if you do not respond, or telling you that you have been a victim of fraud.

Asks you to provide personal information, such as your bank account number, an account password, credit card number, PIN number, mother's maiden name, or Social Security number.

Contains links that do not go where the link text says it will go (point to a hyperlink in the e-mail message to view the URL for that link).

Uses legitimate logos from the company the phisher is posing as.

Appears to come from a known organization, but one you may not have an association with.

Appears to be text or text and images but is actually a single image; it has been created that way to avoid being caught in a spam filter (a program that sorts e-mail based on legitimate e-mail and suspected spam) since spam filters cannot read text that is part of an image in an e-mail message.

Contains spelling or grammatical errors.

TIPS FOR AVOIDING IDENTITY THEFT

Protect your Social Security number—give it out only when necessary.

Be careful with your physical mail and trash—shred all documents containing sensitive data.

Secure your computer—update your operating system and use up-to-date security (antivirus, antispyware, firewall, etc.) software.

Be cautious—never click on a link in an e-mail message or respond to a too-good-to-be-true offer.

Use strong passwords for your computer and online accounts.

Verify sources before sharing sensitive information—never respond to e-mail or phone requests for sensitive information.

Be vigilant while on the go—safeguard your wallet, mobile phone, and portable computer.

Watch your bills and monitor your credit reports—react immediately if you suspect fraudulent activity.

Use security software or browser features that warn you if you try to view a known phishing site.

FIGURE 9-23
Tips to reduce your risk of identity theft.

TIP

You can order your free credit reports online quickly and easily via Web sites like *AnnualCreditReport.com*.

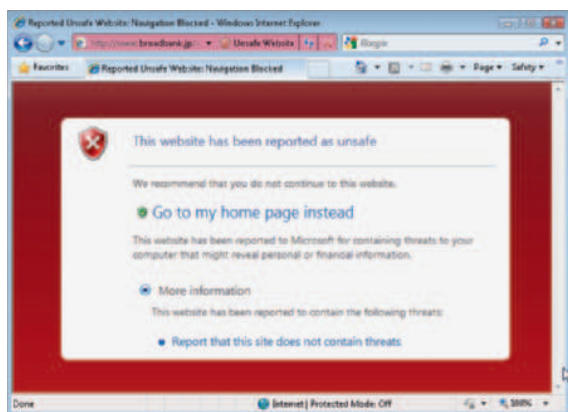
Make sure your bills come in every month (some thieves will change your mailing address to delay detection), and read credit card statements carefully to look for unauthorized charges. Be sure to follow up on any calls you get from creditors, instead of assuming it is just a mistake. Most security experts also recommend ordering a full credit history on yourself a few times a year to check for accounts listed in your name that you did not open and any other problems. The *Fair and Accurate Credit Transactions Act (FACTA)* enables all Americans to get a free copy of their credit report, upon request, each year from the three major consumer credit bureaus. Ideally, you should request a report from one of these bureaus every four months to monitor your credit on a regular basis. These reports contain information about inquiries related to new accounts requested in your name, as well as any delinquent balances or other negative reports. For another tool that you can use to help detect identity theft—*online financial alerts*—see the Technology and You box. You can also use browser-based *antiphishing* tools and *digital certificates* to help guard against identity theft and the phishing and pharming schemes used in conjunction with identity theft, as discussed next. Some additional tips for minimizing your risk of identity theft are listed in Figure 9-23.

Antiphishing Tools

Antiphishing tools are built into many e-mail programs and Web browsers to help notify users of possible phishing Web sites. For instance, some e-mail programs will disable links in e-mail messages identified as questionable, unless the user overrides it; many recent browsers warn users when a Web page associated with a possible phishing URL is requested (see Figure 9-24); and antiphishing capabilities are included in many recent security suites.

In addition, some secure Web sites are adding additional layers in security to protect against identity thieves. For example, some online banking sites analyze users' habits to look for patterns that vary from the norm, such as accessing accounts online at an hour unusual for that individual or a higher than normal level of online purchases. If a bank suspects the account may be compromised, it contacts the owner for verification. Bank of America and some other financial institutions have also added an additional step in their logon process—displaying an image or word preselected by the user and stored on the bank's server—to prove to the user that the site being viewed is the legitimate (not a phishing) site. In addition, if the system does not recognize the

FIGURE 9-24
Unsafe Web site alerts.



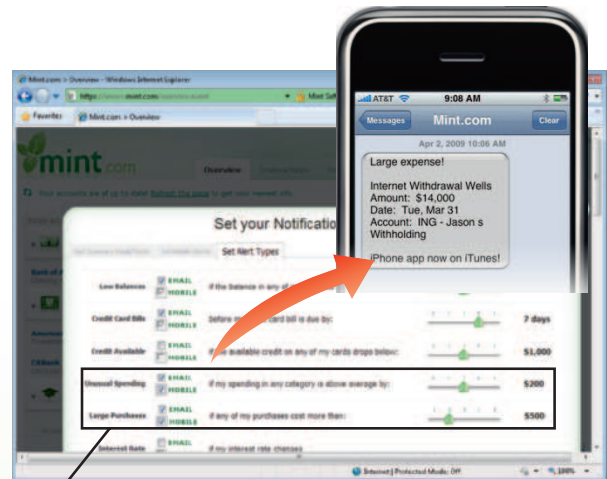
TECHNOLOGY AND YOU

Online Financial Alerts

Want to know as soon as possible when a transaction that might be fraudulent is charged to your credit card? Well, *online financial alerts* might be the answer.

Many online banking services today allow users to set up e-mail alerts for credit card activity over a certain amount, low balances, and so forth. For individuals wishing to monitor multiple accounts, however, online money management aggregator services (such as *Mint.com*) make it easier. Once you have set up a free *Mint.com* account with your financial accounts (including credit cards and checking, savings, and PayPal accounts) and their respective passwords, you can see the status of all your accounts through the *Mint.com* interface. You can also set up alerts for any of the accounts based on your desired criteria, such as any transaction over a specified amount (see the accompanying illustration). The alerts are sent to you via e-mail or text message, depending on your preference, to help notify you as soon as possible if a suspicious activity occurs. And timeliness is of the essence, because the sooner identity theft is discovered, the less time the thief has to make additional fraudulent transactions. For security purposes, *Mint.com* doesn't store online banking usernames and passwords;

instead, a secure online financial services provider is used to connect *Mint.com* to the appropriate financial institutions as needed to update your activity. In addition, the *Mint.com* Web site cannot be used to move money out of or between financial accounts—it can be used only to view information.



Unusual Spending and Large Purchases alerts can help you detect fraudulent charges to your financial accounts.

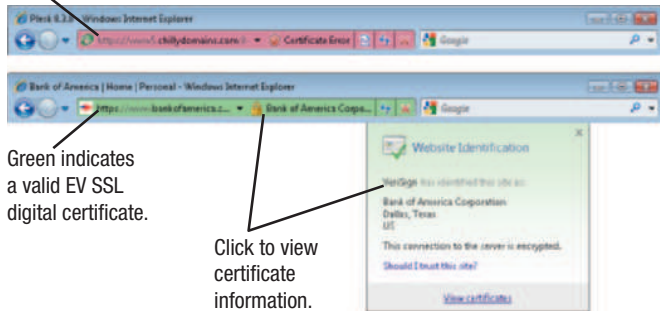
computer that the user is using to log on to the system, the user is required to go through an authentication process (typically by correctly answering cognitive authentication questions) before being allowed to access the system via that computer. The questions used are specifically designed to be “out of wallet” questions—easy for the individual to answer but difficult for hackers to guess the correct answer or find in a stolen wallet. Bank of America is also one bank offering customers the option of adding the use of one-time passwords (autogenerated by a security token like the one shown in Figure 9-5 or sent via text message to the individual’s mobile phone) to their online banking login procedure.

Digital Certificates and Digital Signatures

The purpose of a **digital certificate** is to authenticate the identity of an individual or organization. Digital certificates are granted by Certificate Authorities and typically contain the name of the person, organization, or Web site being certified along with a certificate serial number and an expiration date. Digital certificates also include a public/private key pair. In addition to being used by the certificate holder to encrypt files and e-mail messages (as discussed earlier in this chapter), these keys and the digital certificate are used with secure Web pages to guarantee the Web pages are secure and actually belong to the stated organization (so users can know for sure who their credit card number or other sensitive data is really being sent to, in order to protect against some online scams).

>**Digital certificate.** A group of electronic data that can be used to verify the identity of a person or organization; includes a key pair that can be used for encryption and digital signatures.

Red indicates a problem with the site's digital certificate.



Green indicates a valid EV SSL digital certificate.

Click to view certificate information.



FIGURE 9-25

EV SSL certificates.

The browser's Address bar reflects information about the digital certificate being used.

Secure Web sites can obtain either a normal *SSL digital certificate* or a newer *Extended Validation (EV) SSL digital certificate* that was developed to provide consumers with a higher level of trust while online. While both digital certificates require an application process, the verification process to obtain an EV SSL digital certificate is more thorough, requiring the use of reputable third-party sources to verify that the company has the right to use the Web site domain name in question and that the business requesting the certificate is authorized to do so. With both types of certificates, individuals can click the secure Web page icon in their browser window to view that site's digital certificate in order to ensure that the certificate is valid and issued to the company associated with the Web site being viewed. If an EV

SSL certificate is used, however, additional information is displayed when the Web site is viewed in an EV-compliant browser, such as recoloring the Address bar green to indicate a site using a valid EV SSL certificate and displaying certificate information in the *Security Status bar* to the right of the Address bar, as shown in Figure 9-25.

The keys included in a digital certificate can also be used to authenticate the identity of a person sending an e-mail message or other document via a **digital signature**. To digitally sign an e-mail message or other document, the sender's private key is used and that key, along with the contents of the document, generates a unique digital signature; consequently, a digital signature is different with each signed document. When a digitally signed document is received, the recipient's computer uses the sender's public key to verify the digital signature. Since the document is signed with the sender's private key (that only the sender should know) and the digital signature will be deemed invalid if even one character of the document is changed after it is signed, digital signatures guarantee that the document was sent by a specific individual and that it was not tampered with after it was signed.

Digital signatures are an important component of the emerging *e-mail authentication systems* (such as the *DomainKeys* system used by Yahoo!, eBay, Google, PayPal, and other companies) that may help prevent some types of online fraud in the future as these systems become more widely used. These systems are designed to authenticate e-mail messages via digital signatures and so can help ISPs block phishing e-mails because messages coming from a participating company must be digitally signed by that company in order to be deemed authentic.

TIP

According to the Electronic Signatures in Global and National Commerce Act, any form of electronic signature is as legally binding as a handwritten signature.

Protecting Against Online Auction Fraud and Other Internet Scams

The best protection against many dot cons is common sense. Be extremely cautious of any unsolicited e-mail messages you receive and realize that if an offer sounds too good to be true, it probably is. You should also be cautious when dealing with individuals online through auctions and other person-to-person activities. Before bidding on an auction item, check out the feedback rating of the seller to see comments written by other auction sellers and buyers. Always pay for auctions and other online purchases using a credit card or an online payment service (such as PayPal) that accepts credit card payments so you can dispute the transaction through your credit card company, if needed. Using an online payment service that bills the charge to your credit card, instead of allowing the seller to charge your credit card, has the extra advantage of keeping your credit card information private.

➤ **Digital signature.** A unique digital code that can be attached to a file or an e-mail message to verify the identity of the sender and guarantee the file or message has not been changed since it was signed.

In addition, some auction sites and online payment services offer free buyer protection against undelivered items or auction items that are significantly different from the description provided in the auction information. For instance, most eBay purchases paid for via PayPal have at least \$200 of buyer protection coverage at no additional cost. For expensive items, consider using an *escrow service*, which allows you to ensure that the merchandise is as specified before your payment is released to the seller.

PERSONAL SAFETY ISSUES

In addition to being expensive and inconvenient, cybercrime can also be physically dangerous. Although most of us may not ordinarily view using the Internet as a potentially dangerous activity, cases of physical harm due to Internet activity do happen. For example, children and teenagers have become the victims of pedophiles who arranged face-to-face meetings by using information gathered via e-mail, message boards, social networking sites, or other online sources. There are also a growing number of incidents in which children are threatened by classmates via e-mail, Web site posts, or text messages. Adults may fall victim to unscrupulous or dangerous individuals who misrepresent themselves online, and the availability of personal information online has made it more difficult for individuals to hide from people who may want to do them harm, such as abused women trying to hide from their abusive husbands. Two of the most common ways individuals are harassed online—*cyberbullying* and *cyberstalking*—are discussed next.

Cyberbullying and Cyberstalking

Children and teenagers bullying other children or teenagers via the Internet—such as through e-mail, a text message, a social networking site, a blog, or other online communications method—is referred to as **cyberbullying**. Unfortunately, cyberbullying is common today—by some estimates, it affects as many as one-half of all U.S. teenagers. Cyberbullying can take place via direct online communication (such as with an e-mail or instant message), as well as via more subtle means. For instance, there have been cases of students posting videos on YouTube of other students being bullied and cases of individuals hacking into a student's MySpace or Facebook account and changing the content on the student's pages to harass that student. In one tragic instance, a 13-year-old girl hanged herself after the mother of one of the girl's classmates arranged to have a MySpace profile created for a nonexistent teenage boy in order to determine what the victim was saying about her daughter, and then cruelly ended the friendship. While the mother was convicted of three misdemeanor charges of unauthorized access to computers in conjunction with the case, her conviction was dismissed in 2009. However, the case prompted many states and schools to look at harassment statutes and bullying policies and resulted in several states implementing new laws or amending existing harassment laws to address cyberbullying.

Repeated threats or other harassment carried out online between adults is referred to as **cyberstalking**. Cyberstalkers sometimes find their victims online; for instance, someone in a discussion group who makes a comment or has a screen name that the cyberstalker does not like, or bloggers who are harassed and threatened with violence or murder because of their blogging activities. Other times, the attack is more personal, such as employers who are stalked online by ex-employees who were fired or otherwise left their position under adverse conditions, and celebrities who are stalked online by fans.

Cyberstalking typically begins with online harassment—such as sending harassing or threatening e-mail messages or unwanted files to the victim, posing as the victim in order to

FURTHER EXPLORATION

Go

Go to the Chapter 9 page at www.cengage.com/computerconcepts/np/uc13 for links to information about how to prevent and deal with identity theft and online auction fraud.

NET

>**Cyberbullying.** Children or teenagers bullying other children or teenagers via the Internet. >**Cyberstalking.** Repeated threats or harassing behavior between adults carried out via e-mail or another Internet communications method.

sign the victim up for pornographic or otherwise offensive e-mail newsletters, publicizing the victim's home address and telephone number, or hacking into the victim's social networking pages to alter the content. Cyberstalking can also lead to offline stalking and possibly physical harm—in at least one case, it led to the death of the victim. While there are as yet no specific federal laws against cyberstalking, all states have made it illegal (and it is being increasingly prosecuted), and some federal laws do apply if the online actions include computer fraud or another type of computer crime, suggest a threat of personal injury, or involve sending obscene e-mail messages. Many cyberstalkers are not caught, however, due in part to the anonymity of the Internet, which assists cyberstalkers in concealing their true identities.

Online Pornography

A variety of controversial and potentially objectionable material is available on the Internet. Although there have been attempts to ban this type of material from the Internet, they have not been successful. For example, the *Communications Decency Act*, signed into law in 1996—which made it a criminal offense to distribute patently indecent or offensive material online—was ruled unconstitutional in 1997 by the U.S. Supreme Court. However, like its printed counterpart, online pornography involving minors is illegal. Because of the strong link they believe exists between child pornography and child molestation, many experts are very concerned about the amount of child pornography that can be found and distributed via the Internet. They also believe that the Internet makes it easier for sexual predators to act out, such as by striking up “friendships” with children online and convincing these children to meet them in real life. And this can have devastating consequences, as it did for a 13-year-old girl from Connecticut who was strangled to death in 2002 by a 25-year-old man she met originally online and eventually in person. Although the man confessed, he maintains that the strangling was accidental. The man was sentenced in late 2003 to a total of 40 years in prison for state and federal charges relating to the crime.

PROTECTING AGAINST CYBERBULLYING, CYBERSTALKING, AND OTHER PERSONAL SAFETY CONCERNS

The growing increase in attention to cyberbullying and cyberstalking is leading to more efforts to improve safeguards for children. For instance, social networking sites have privacy features that can be used to protect the private information of their members. In addition, numerous states in the U.S. have implemented cyberbullying and cyberstalking laws. While there is no surefire way to protect against cyberbullying, cyberstalking, and other online dangers completely, some common-sense precautions can reduce the chance of a serious personal safety problem occurring due to online activities.

TIP

Search for yourself using search sites and online telephone books to see what personal information is available about you on the Internet.

TIP

Both adults and children should avoid including personal information on social networking sites that could be used by an online stalker.

Safety Tips for Adults

It is wise to be cautious and discreet online—especially in online profiles, message boards, and other online locations where individuals communicate with strangers. To protect yourself against cyberstalking and other types of online harassment, use gender-neutral, nonprovocative identifying names, such as *jsmith*, instead of *janesmith* or *iamcute*. Be careful about the types of photos you post of yourself online and do not reveal personal information—such as your real name, address, or telephone number—to people you meet online. In addition, do not respond to any insults or other harassing comments you may receive online. You may also wish to request that your personal information be removed from online directories—especially those associated with your e-mail address or other online identifiers.

Safety Tips for Children and Teens

Most experts agree that the best way to protect children from online dangers is to stay in close touch with them as they explore the Internet. In order for parents to be able to monitor

their children's online activities, children and teenagers should use a computer in a family room or other public location, instead of their bedroom, and they should be told which activities are allowed, which types of Web sites are off-limits, and why. In addition, it should be made clear that they are never to reveal personal information about themselves online without a parent's permission. They should also be instructed to tell a parent (or teacher if at school) if an individual ever requests personal information or a personal meeting, or threatens or otherwise harasses the child, via any type of online communications medium. Older children should also be cautioned about sending compromising photos of themselves to others. This practice—referred to as *sexting*—is a growing problem. In one recent study, for instance, more than 20% of teens reported sending nude or seminude photos of themselves to others. Part of the problem is that many young people don't realize they lose control of photos and other compromising content once that information has been sent to others and, in one case, a teenage girl committed suicide after the nude photos she had sent her boyfriend were sent to other students once the couple broke up. Sexting has also resulted in child pornography charges being filed against teens for sending their own photos to others or having compromising photos of other children on their mobile phones.

NETWORK AND INTERNET SECURITY LEGISLATION

Although new legislation is passed periodically to address new types of computer crimes, it is difficult for the legal system to keep pace with the rate at which technology changes. In addition, there are both domestic and international jurisdictional issues because many computer crimes affect businesses and individuals located in geographic areas other than the one in which the computer criminal is located, and hackers can make it appear that activity is coming from a different location than it really is. Nevertheless, computer crime legislation continues to be proposed and computer crimes are being prosecuted. A list of selected federal laws concerning network and Internet security is shown in Figure 9-26.

FIGURE 9-26
Computer network
and Internet security
legislation.

DATE	LAW AND DESCRIPTION
2004	Identity Theft Penalty Enhancement Act Adds extra years to prison sentences for criminals who use identity theft (including the use of stolen credit card numbers) to commit other crimes, including credit card fraud and terrorism.
2003	CAN-SPAM Act Implements regulations for unsolicited e-mail messages.
2003	Fair and Accurate Credit Transactions Act (FACTA) Amends the Fair Credit Reporting Act (FCRA) to require, among other things, that the three nationwide consumer reporting agencies (Equifax, Experian, and TransUnion) provide to consumers, upon request, a free copy of their credit report once every 12 months.
2003	PROTECT Act Includes provisions to prohibit virtual child pornography.
2003	Health Insurance Portability and Accountability Act (HIPAA) Includes a Security Rule that sets minimum security standards to protect health information stored electronically.
2002	Homeland Security Act Includes provisions to combat cyberterrorism, including protecting ISPs against lawsuits from customers for revealing private information to law enforcement agencies.
2002	Sarbanes-Oxley Act Requires archiving a variety of electronic records and protecting the integrity of corporate financial data.
2001	USA PATRIOT Act Grants federal authorities expanded surveillance and intelligence-gathering powers, such as broadening the ability of federal agents to obtain the real identity of Internet users, intercept e-mail and other types of Internet communications, follow online activity of suspects, expand their wiretapping authority, and more.
1998	Identity Theft and Assumption Deterrence Act of 1998 Makes it a federal crime to knowingly use someone else's means of identification, such as name, Social Security number, or credit card, to commit any unlawful activity.
1997	No Electronic Theft (NET) Act Expands computer piracy laws to include distribution of copyrighted materials over the Internet.
1996	National Information Infrastructure Protection Act Amends the Computer Fraud and Abuse Act of 1984 to punish information theft crossing state lines and to crack down on network trespassing.
1994	Computer Abuse Amendments Act Amends the Computer Fraud and Abuse Act of 1984 to include computer viruses and other harmful code.
1986	Computer Fraud and Abuse Act of 1986 Amends the 1984 law to include federally regulated financial institutions.
1984	Computer Fraud and Abuse Act of 1984 Makes it a crime to break into computers owned by the federal government. This act has been regularly amended over the years as technology has changed.

SUMMARY

Chapter Objective 1:

Explain why computer users should be concerned about network and Internet security.

Chapter Objective 2:

List several examples of unauthorized access and unauthorized use.

Chapter Objective 3:

Explain several ways to protect against unauthorized access and unauthorized use, including access control systems, firewalls, and encryption.

Chapter Objective 4:

Provide several examples of computer sabotage.

Chapter Objective 5:

List how individuals and businesses can protect against computer sabotage.

WHY BE CONCERNED ABOUT NETWORK AND INTERNET SECURITY?

There are a number of important security concerns related to computers and the Internet. Many of these are **computer crimes**. Because computers and networks are so widespread and many opportunities for criminals exist, all computer users should be aware of the risks of using networks and the Internet so they can take appropriate precautions.

UNAUTHORIZED ACCESS AND UNAUTHORIZED USE

Two risks related to networks and the Internet are **unauthorized access** and **unauthorized use**. **Hacking** is using a computer to break into a computer. **War driving** and **Wi-Fi piggybacking** refer to the unauthorized use of unsecured Wi-Fi network. Data can be intercepted as it is transmitted over the Internet or a wireless network.

PROTECTING AGAINST UNAUTHORIZED ACCESS AND UNAUTHORIZED USE

Access control systems are used to control access to a computer, network, or other resource. These include **possessed knowledge access systems** that use **passwords** or other types of possessed knowledge; **possessed object access systems** that use physical objects; and **biometric access systems** that identify users by a particular unique biological characteristic, such as a fingerprint. Passwords should be *strong passwords*; **two-factor authentication systems** that use multiple factors are more effective than single-factor systems.

To protect wireless networks, they should be secured; **firewalls** protect against unauthorized access. Sensitive transactions should be performed only on **secure Web pages**; sensitive files and e-mails should be secured with **encryption**. **Public key encryption** uses a private key and matching public key; **private key encryption** uses only a private key. A **virtual private network (VPN)** can be used to provide a secure remote connection to a company network, as well as to protect individuals at public Wi-Fi hotspots. Employers should take appropriate precautions with current and former employees to limit the risk of unauthorized access and use, as well as accidental exposure of sensitive information.

COMPUTER SABOTAGE

Computer sabotage includes **malware** (**computer viruses**, **computer worms**, and **Trojan horses** designed to cause harm to computer systems), **denial of service (DoS) attacks** (designed to shut down a Web server), and data and program alteration. Computer sabotage is often performed via the Internet, increasingly by the **bots** in a **botnet**.

PROTECTING AGAINST COMPUTER SABOTAGE

Protection against computer sabotage includes using appropriate access control systems to keep unauthorized individuals from accessing computers and networks, as well as using **security software**. In particular, **antivirus software** protects against computer viruses and other types of malware. It is important to keep your security software up to date.

ONLINE THEFT, ONLINE FRAUD, AND OTHER DOT CONS

There are a variety of types of theft, fraud, and scams related to the Internet—collectively referred to as **dot cons**—that all Internet users should be aware of. Data, information, or money can be stolen from individuals and businesses. A common crime today is **identity theft**, in which an individual poses as another individual—typically to steal money or make purchases posing as the victim. The information used in identity theft is often gathered via **phishing**, **spear phishing**, and **pharming**. **Online auction fraud** is another common dot con.

PROTECTING AGAINST ONLINE THEFT, ONLINE FRAUD, AND OTHER DOT CONS

To protect against identity theft, individuals should guard their personal information carefully. To check for identity theft, watch your bills and credit history. When interacting with other individuals online or buying from an online auction, it is wise to be conservative and use a credit card whenever possible. To avoid other types of dot cons, be very wary of responding to unsolicited offers and e-mails, and steer clear of offers that seem too good to be true. Never click a link in an e-mail message to update your personal information. To verify a Web site, a **digital certificate** can be used. To verify the sender of a document, a **digital signature** can be used. Digital certificates include key pairs that can be used to both digitally sign documents and to encrypt files.

PERSONAL SAFETY ISSUES

There are also personal safety risks for both adults and children stemming from Internet use. **Cyberbullying** and **cyberstalking**—online harassment that frightens or threatens the victim—is more common in recent years, even though most states have passed laws against it. Cyberbully is a growing risk for children, as is the potential exposure to online pornography and other materials inappropriate for children, and the growing *sexting* trend.

PROTECTING AGAINST CYBERBULLYING, CYBERSTALKING, AND OTHER PERSONAL SAFETY CONCERNS

To protect their personal safety, adults and children should be cautious in online communications. They should be wary of revealing any personal information or meeting online acquaintances in person. To protect children, parents should keep a close watch on their children's online activities, and children should be taught never to reveal personal information to others online without a parent's consent.

NETWORK AND INTERNET SECURITY LEGISLATION

The rapid growth of the Internet and jurisdictional issues have contributed to the lack of network and Internet security legislation. However, computer crime legislation continues to be proposed and computer crimes are actively prosecuted.

Chapter Objective 6:

Discuss online theft, identity theft, spoofing, phishing, and other types of dot cons.

Chapter Objective 7:

Detail steps an individual can take to protect against online theft, identity theft, spoofing, phishing, and other types of dot cons.

Chapter Objective 8:

Identify personal safety risks associated with Internet use.

Chapter Objective 9:

List steps individuals can take to safeguard their personal safety when using the Internet.

Chapter Objective 10:

Discuss the current state of network and Internet security legislation.