Understanding Computers in a Changing Society

5e

Deborah Morley

Chapter 4 Securing Your Network and Internet Connections

Learning Objectives

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.

Learning Objectives

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.

Overview

- This chapter covers:
  - Security concerns stemming from the use of computer networks and the Internet in our society
  - Safeguards and precautions that can be taken to reduce the risk of problems related to these security concerns
  - Personal safety issues related to the Internet

Why Be Concerned About Network and Internet Security?

- Security concerns related to computer networks and the Internet abound
- Computer Crime (cybercrime)
  - Any illegal act involving a computer, including:
    - Theft of financial assets
    - Manipulating data for personal advantage
    - Act of sabotage (releasing a computer virus, shutting down a Web server)
    - Phishing and Internet scams
- All computer users should be aware of security concerns and the precautions that can be taken

Unauthorized Access and Unauthorized Use

- Unauthorized Access
  - Gaining access to a computer, network, file, or other resource without permission
- Unauthorized Use
  - Using a computer resource for unapproved activities
- Both can be committed by insiders and outsiders
- Codes of Conduct
  - Used to specify rules for behavior, typically by a business or school

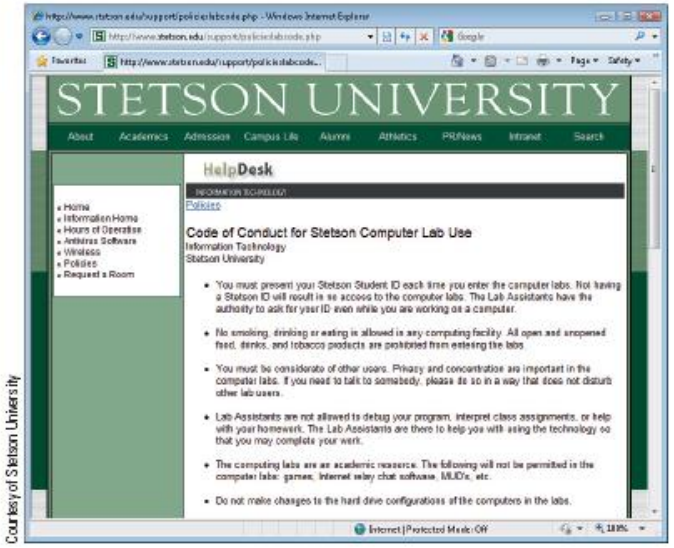


FIGURE 4-1
A sample code of conduct.

Unauthorized Access and Unauthorized Use

- Hacking
  - Using a computer to break into another computer system
    - A serious threat for individuals, businesses, and the country (national security), i.e., cyberterrorism
    - Often performed via wireless networks today
      - 70% of wireless networks are left unsecured
- War Driving and Wi-Fi Piggybacking
  - War Driving
    - Driving around an area to find a Wi-Fi network to access and use without authorization

Unauthorized Access and Unauthorized Use

- Wi-Fi Piggybacking
  - Accessing an unsecured Wi-Fi network from the hacker's current location without authorization
- Interception of Communications
  - Unsecured messages, files, logon information, etc., can be intercepted using software designed for that purpose
  - New trend is to intercept credit and debit card information during the card verification process
    - Packetsniffing software

FIGURE 4-2
Wi-Fi finders. Online mapping services and smartphone apps can show you the available Wi-Fi hotspots for a particular geographic area.

Courtesy of JiWire

Protecting Against Unauthorized Access and Unauthorized Use

- Access Control Systems
  - Used to control access to facilities, computer networks, databases, and Web site accounts
    - Identification Systems
      - Verify that the person trying to access the facility or system is an authorized user
    - Authentication Systems
      - Determine if the person is who he or she claims to be

Protecting Against Unauthorized Access and Unauthorized Use

- Possessed Knowledge Access Systems
  - Use information that only the authorized user should know
    - Passwords should be strong and changed frequently
    - Typically used in conjunction with usernames
  - Disadvantages
    - Passwords can be forgotten
    - If known, password can be used by someone who is not an authorized user

FIGURE 4-3
Passwords.
Passwords are used to log on to computers, networks, Web sites, and other computing resources.

Protecting Against Unauthorized Access and Unauthorized Use

- Cognitive Authentication Systems
  - Use information the individual knows or can easily remember (birthplace, pet names, etc.)
  - Used in many password recovery systems
- Two-factor Authentication
  - Using two different methods to authenticate users
    - » Biometric Feature – something you are
    - » Possessed Object – something you have
    - » Conventional username/password combination in conjunction with an access card that contains a one-time password

Protecting Against Unauthorized Access and Unauthorized Use

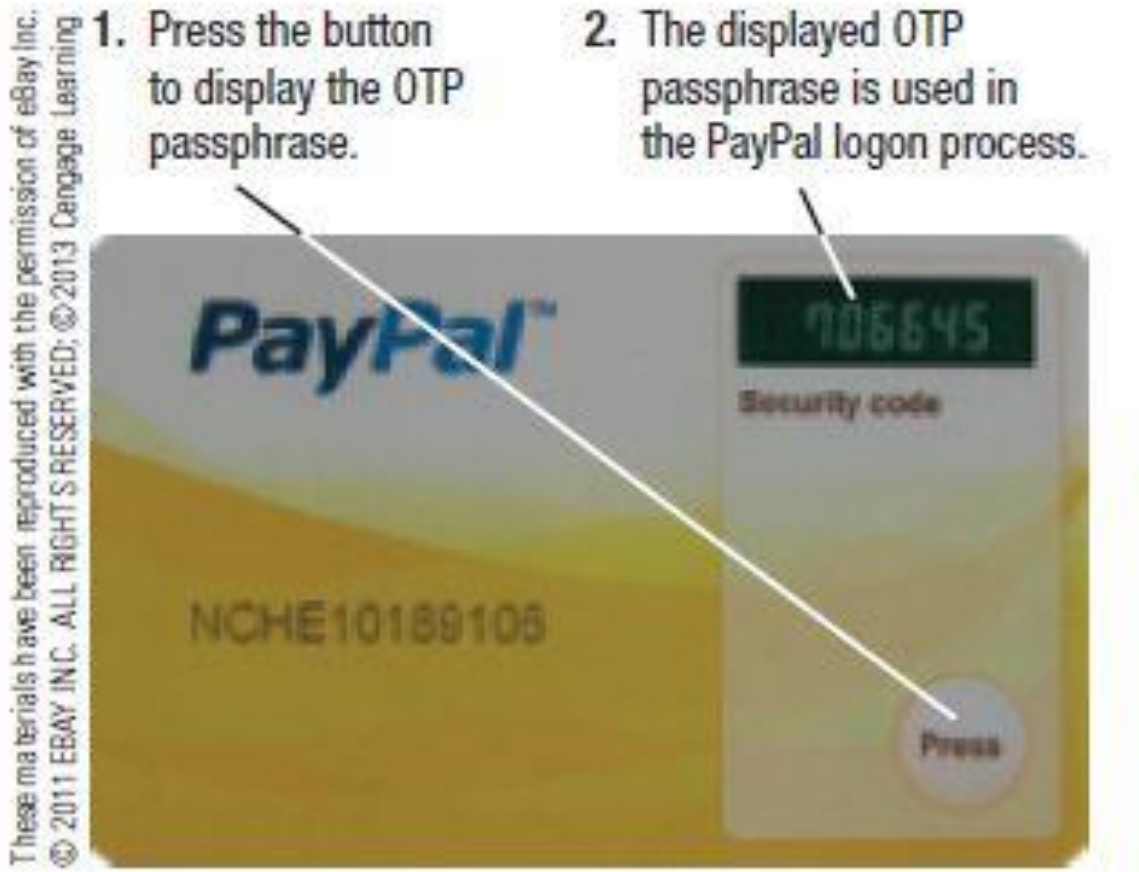


FIGURE 4-5
Two-factor authentication. With this system, the user must have both the access card (to obtain the OTP) and his or her conventional username/password combination, in order to log on to his or her online account.

Protecting Against Unauthorized Access and Unauthorized Use

- Possessed Object Access Systems
  - Use a physical object an individual has in his/her possession to identify that individual
  - Smart cards, magnetic cards
  - RFID-encoded badges, USB security keys or e-tokens

Courtesy ActivIdentity

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

Joseph Mehling, Dartmouth College

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

FIGURE 4-6
Possessed objects.
Help protect against unauthorized access; some can also store additional security credentials.

Protecting Against Unauthorized Access and Unauthorized Use

- Disadvantages
  - Can be lost or used by an unauthorized individual

– Biometric Access Systems
  - Identifies users by a particular unique biological characteristic
    - Fingerprint, hand, face, iris, voice, etc.
  - Data read by biometric reader must match what is stored in a database

Protecting Against Unauthorized Access and Unauthorized Use

- Often used to
  - Control access to secure facilities
  - Log on to computers, punch in/out at work, law enforcement, etc.
- Advantages
  - Can only be used by the authorized individual
  - Cannot be lost or forgotten
- Disadvantages
  - Cannot be reset if compromised
  - Hardware and software are expensive

Protecting Against Unauthorized Access and Unauthorized Use

pmphoto/Shutterstock.com

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

Courtesy Ingersoll Rand Security Technologies

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

Sean Nel/Shutterstock.com; Courtesy of Luxand, Inc.

FACE RECOGNITION SYSTEMS
Typically used to control access to highly secure areas, to identify individuals for law enforcement purposes, and to log on to computers, as shown here.

Courtesy of Susan Huseman (USAG Stuttgart)

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 4-7
Types of biometric access and identification systems.

Protecting Against Unauthorized Access and Unauthorized Use

- Controlling Access to Wireless Networks
  - In general, Wi-Fi is less secure than wired networks
  - Security is usually off by default; wireless networks should be secured
  - Wireless network owners should:
    - Enable encryption (WPA is more secure than WEP)
    - Not broadcast the network name (SSID)
    - Enable other security features as needed

Protecting Against Unauthorized Access and Unauthorized Use

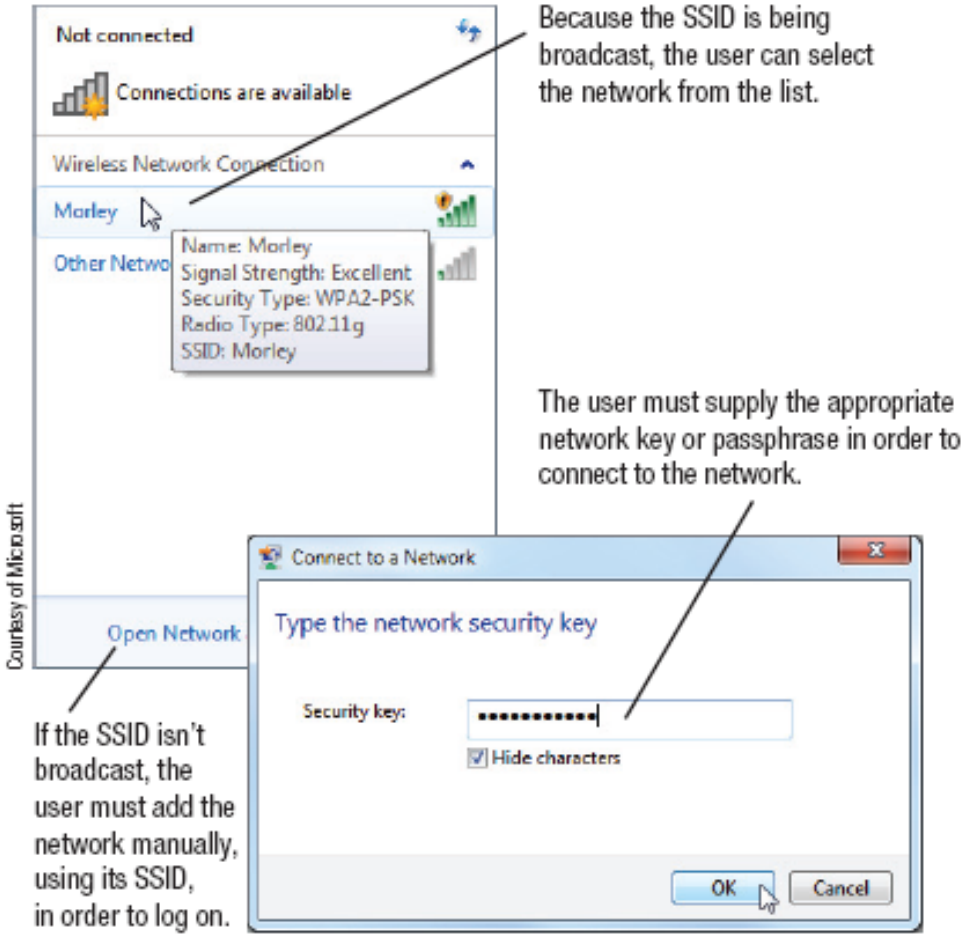


FIGURE 4-8
Accessing a Wi-Fi network. To access a secure network, the appropriate passphrase must be supplied.

Protecting Against Unauthorized Access and Unauthorized Use

- Firewalls, Encryption, and Virtual Private Networks (VPNs)
  - Firewalls
    - A collection of hardware and/or software intended to protect a computer or computer network from unauthorized access
    - Block access to the computer from hackers
    - Block access to the Internet from programs on the user's computer unless authorized by the user
    - Important for home computers that have a direct Internet connection, as well as for businesses
    - Work by closing down external communications ports

Protecting Against Unauthorized Access and Unauthorized Use

- Intrusion Prevention System (IPS) Software
  - Monitors traffic to try and detect possible attacks
  - If an attack is discovered, IPS software can immediately block it

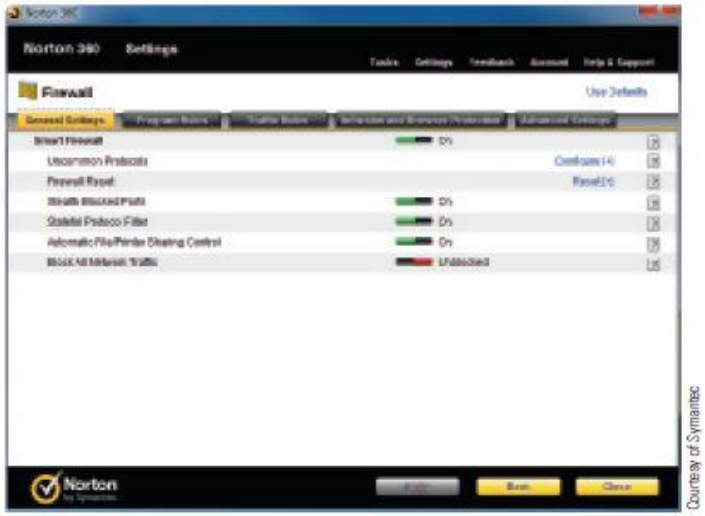


FIGURE 4-9
A personal firewall.

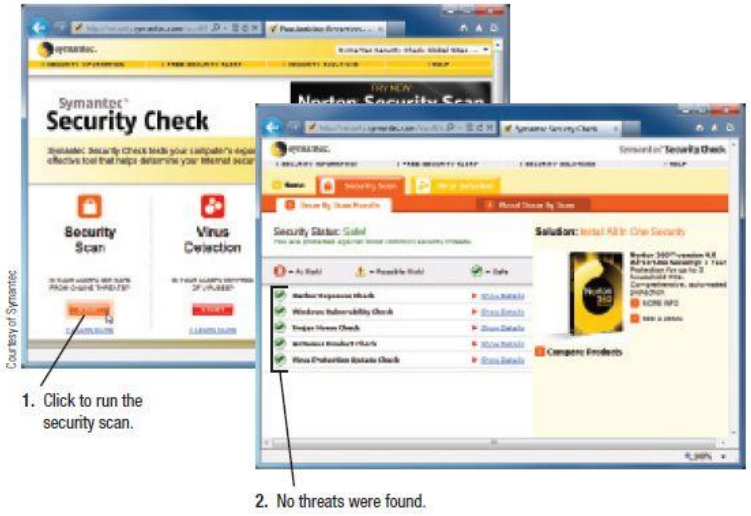


FIGURE 4-10
Online security scans can check your system for vulnerabilities.

Protecting Against Unauthorized Access and Unauthorized Use

- Encryption
  - Method of scrambling contents of e-mail or files to make them unreadable if intercepted
  - Private Key Encryption (symmetric key encryption)
    - Uses a single key
    - Most often used to encrypt files on a computer
    - If used to send files to others, the recipient and sender must agree on the private key to be used

Protecting Against Unauthorized Access and Unauthorized Use

- Public Key Encryption (asymmetric key encryption)
  - Uses two keys (a private key and a public key) to encrypt and decrypt documents
  - Public key can be given to anyone
  - Key pairs can be obtained through a Certificate Authority
- Web-based encrypted e-mail (HushMail) is available

Protecting Against Unauthorized Access and Unauthorized Use

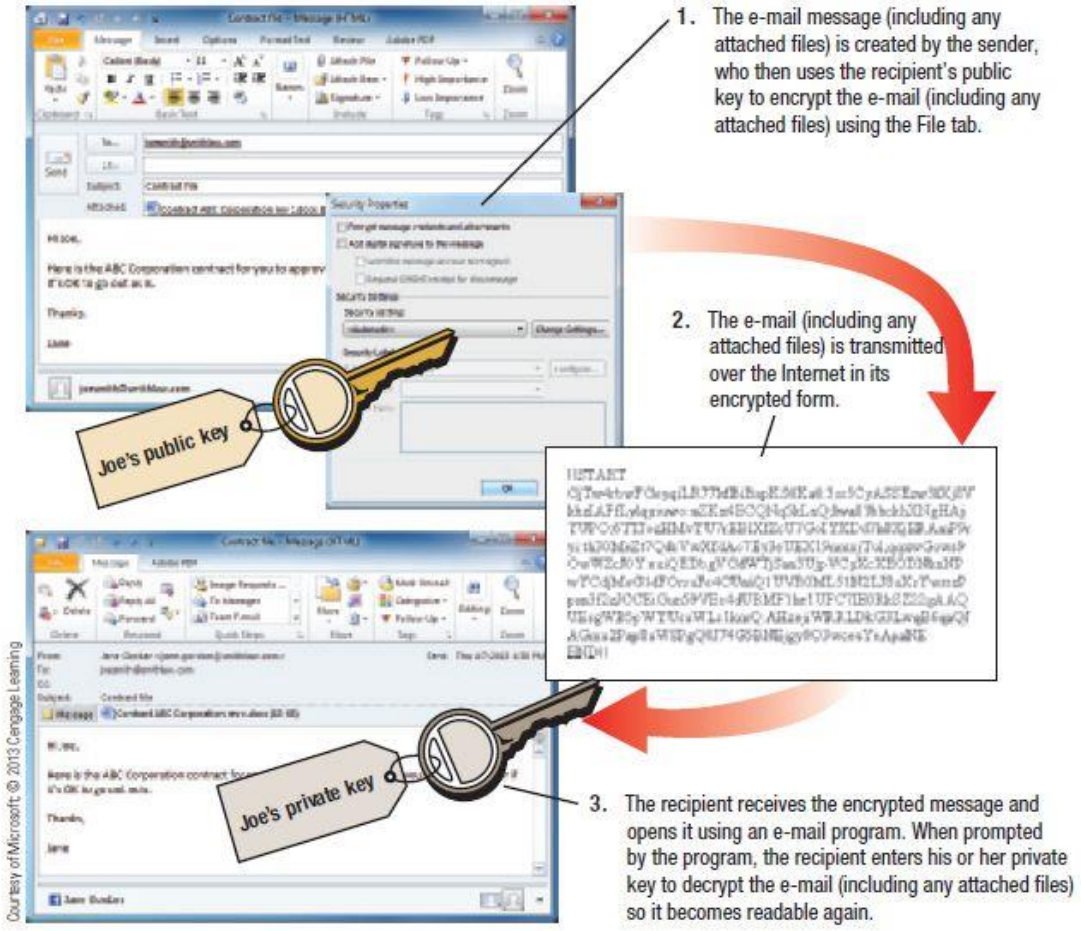


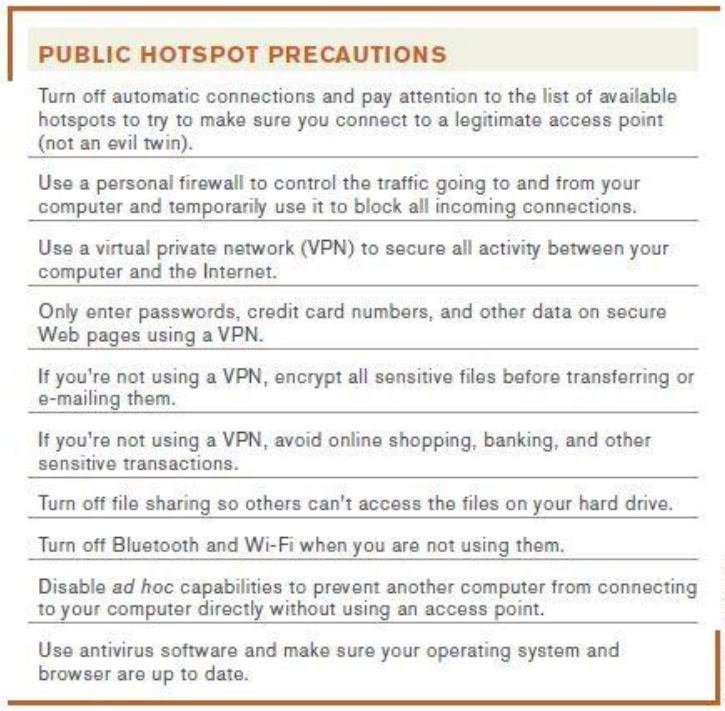
FIGURE 4-11
Using public key encryption to secure an e-mail message.

Protecting Against Unauthorized Access and Unauthorized Use

- Virtual Private Networks (VPNs)
  - A private secure path over the Internet
  - Allows authorized users to securely access a private network via the Internet
  - Much less expensive than a private secure network since it uses the Internet
  - Can provide a secure environment over a large geographical area
  - Typically used by businesses to remotely access corporate networks via the Internet
  - Personal VPNs can be used by individuals to surf safely at a wireless hotspot

Protecting Against Unauthorized Access and Unauthorized Use

- Additional Public Hotspot Precautions
  - Individuals should take additional precautions when using public hotspots in addition to using security software, secure Web pages, VPNs, and file encryption



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 and browser are up to date.

FIGURE 4-12 Sensible precautions for public Wi-Fi hotspot users.

Quick Quiz

1. Which of the following is an example of possessed knowledge?
   a. Password
   b. Smart card
   c. Fingerprint
2. True or False: With public key encryption, a single key is used to both encrypt and decrypt the file.
3. A(n) _____ controls access to a computer from the Internet and protects programs installed on a computer from accessing the Internet without authorization from the user.

Answers:

1) a; 2) False; 3) firewall

Computer Sabotage

- Computer Sabotage
  - Acts of malicious destruction to a computer or computer resource
    - Launching a computer virus
    - Denial of Service attack
  - Botnet
    - A group of bots (computers controlled by a hacker) that are controlled by one individual and work together in a coordinated fashion
    - Used by botherders (criminals) to send spam, launch Internet attacks and malware, etc.

Computer Sabotage

- Computer Viruses and Other Types of Malware
  - Malware
    - Any type of malicious software
    - Written to perform destructive acts (damaging programs, deleting files, erasing drives, etc.)
      - Logic bomb
      - Time bomb
    - Writing malware is considered unethical; distributing is illegal
    - Can infect mobile phones and mobile devices (some preinstalled on mobile devices)

Computer Sabotage

- Computer Viruses
  - 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
  - Often embedded in downloaded programs and e-mail messages (games, videos, music files)
- Computer Worm
  - Malicious program designed to spread rapidly by sending copies of itself to other computers via a network
  - Typically sent as an e-mail attachment

Computer Sabotage

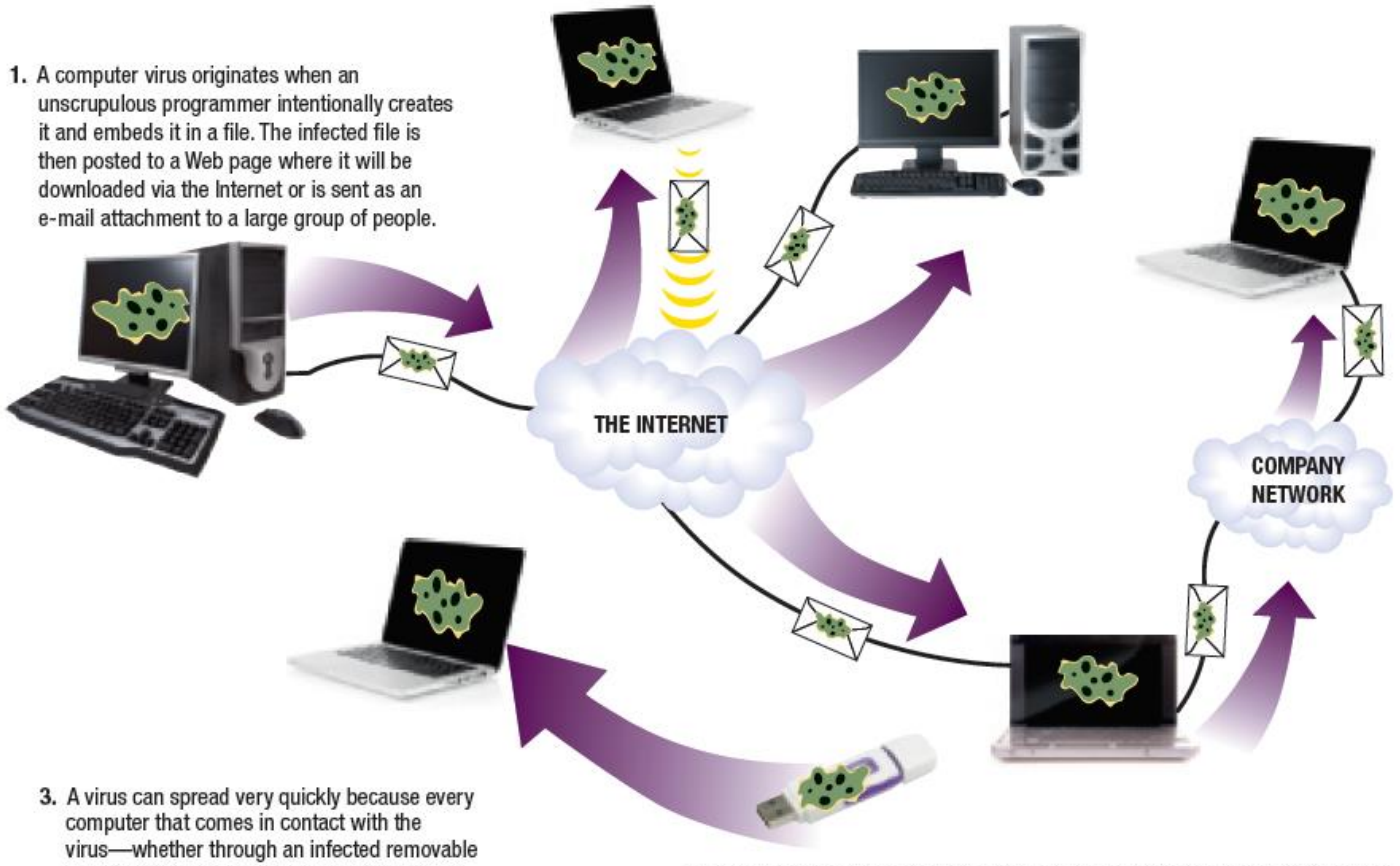


FIGURE 4-14
How a computer virus or other type of malicious software might spread.

300dpi/Shutterstock.com; Evgeny Karandaev/Shutterstock.com; karam Miri/Shutterstock.com; FikMik/Shutterstock.com; Courtesy Kingston Technology Company, Inc.

Computer Sabotage

- Trojan Horse
  - Malicious program that masquerades as something else
  - Usually appears to be a game or utility program
  - Cannot replicate themselves; must be downloaded and installed
  - Rogue antivirus programs are common today

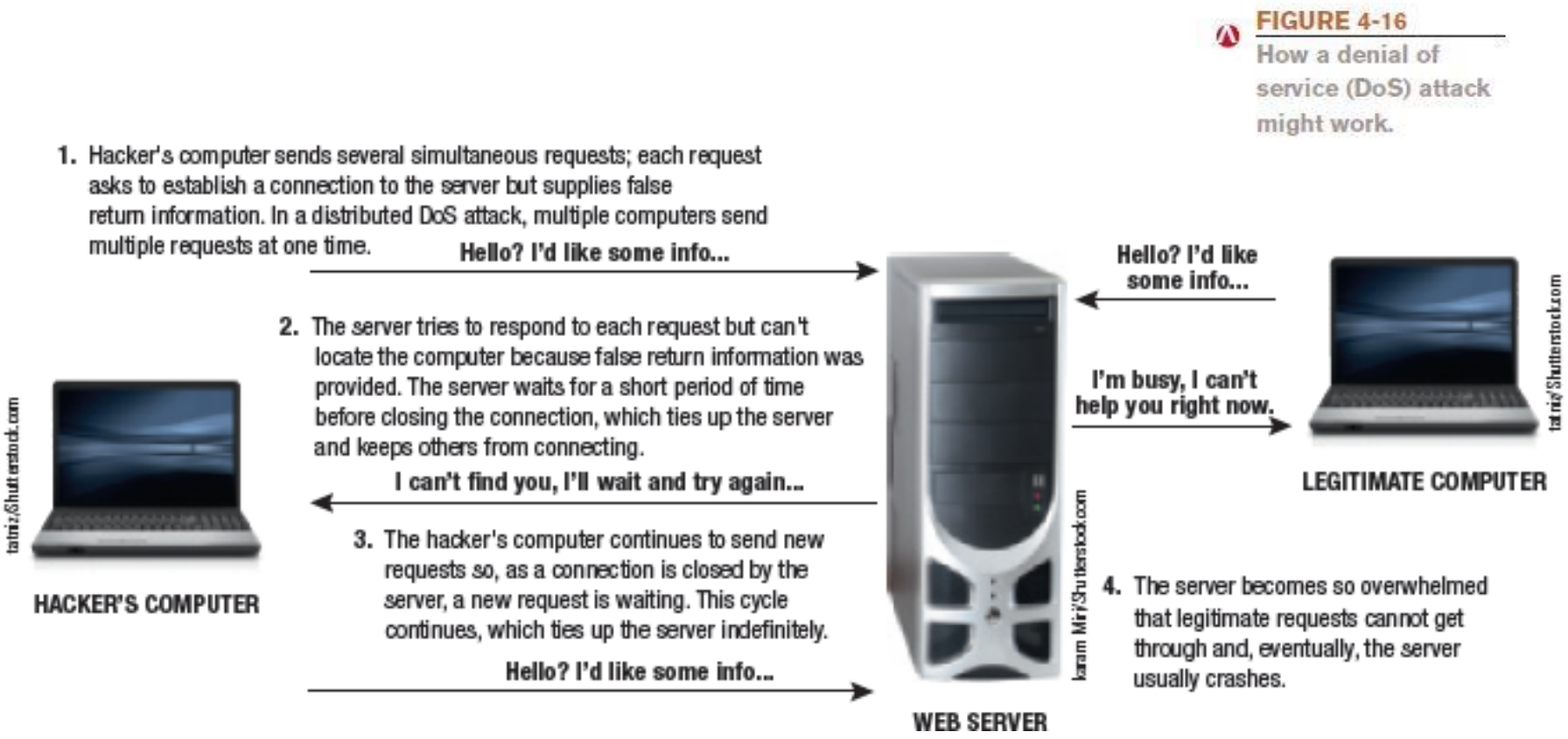
Courtesy of How-to-Geek

FIGURE 4-15
Rogue anti-malware programs. These programs try to trick victims into purchasing subscriptions to remove nonexistent malware supposedly installed on their computers.

Computer Sabotage

- Mobile Malware
  - Can infect mobile phones, portable digital media, players, printers, etc.
  - Mobile phones with Bluetooth are particularly vulnerable to attack
  - Mobile threats are expected to continue to increase
- Denial of Service (DoS) Attacks
  - Act of sabotage that attempts to flood a network server or Web server with so much activity that it is unable to function
  - Distributed DoS Attacks target popular Web sites (like Twitter) and use multiple computers

Computer Sabotage



Computer Sabotage

- Data, Program, or Web Site Alteration
  - Sabotage occurs when a hacker breaches a computer system in order to delete/change data or modify programs
    - Student changing grades
    - Employee performing vengeful acts, such as deleting or changing corporate data
  - Data on Web sites can also be altered
    - Web sites defaced to make political statements
    - Hacking into and changing social networking account contents (Facebook pages, Twitter tweets, etc.)
    - Altering legitimate site to perform malware attacks

Protecting Against Computer Sabotage

- Security Software
  - Typically a suite of programs used to protect your computer against a variety of threats
  - Antivirus Software
    - Used to detect and eliminate computer viruses and other types of malware
    - Should be set up to run continuously to check incoming e-mail messages, instant messages, Web page content, and downloaded files
    - Quarantines any suspicious content as it arrives
    - Should be set to perform regular system scans

Protecting Against Computer Sabotage

- Download new virus definitions on a regular basis as new malware is introduced all the time

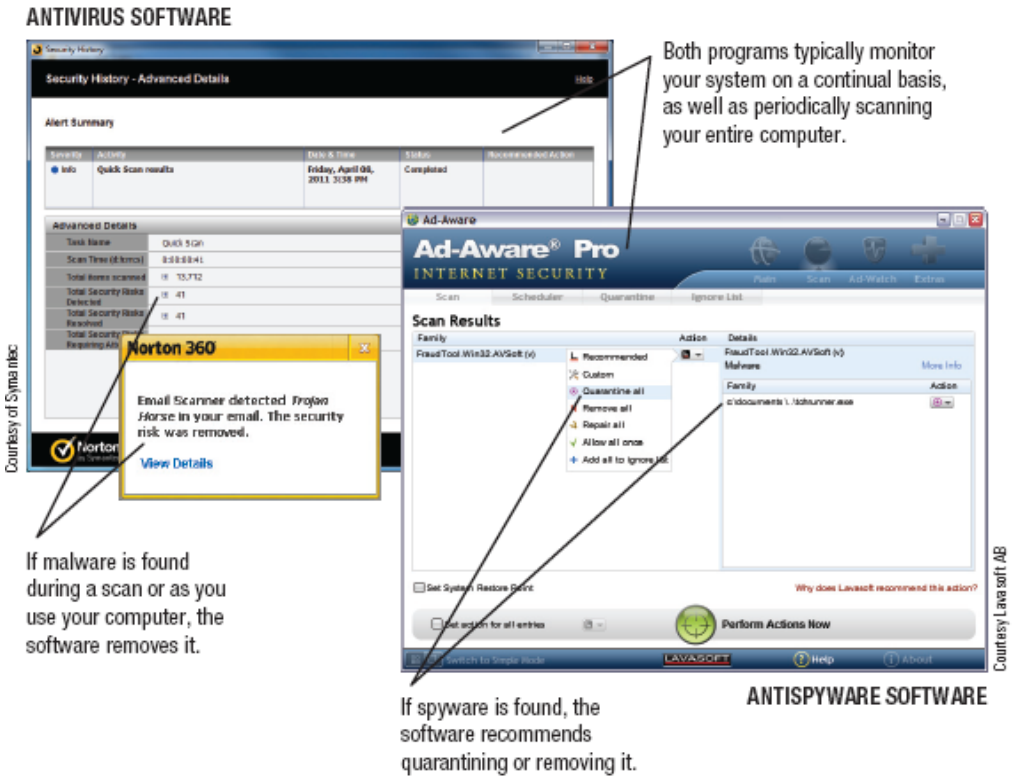
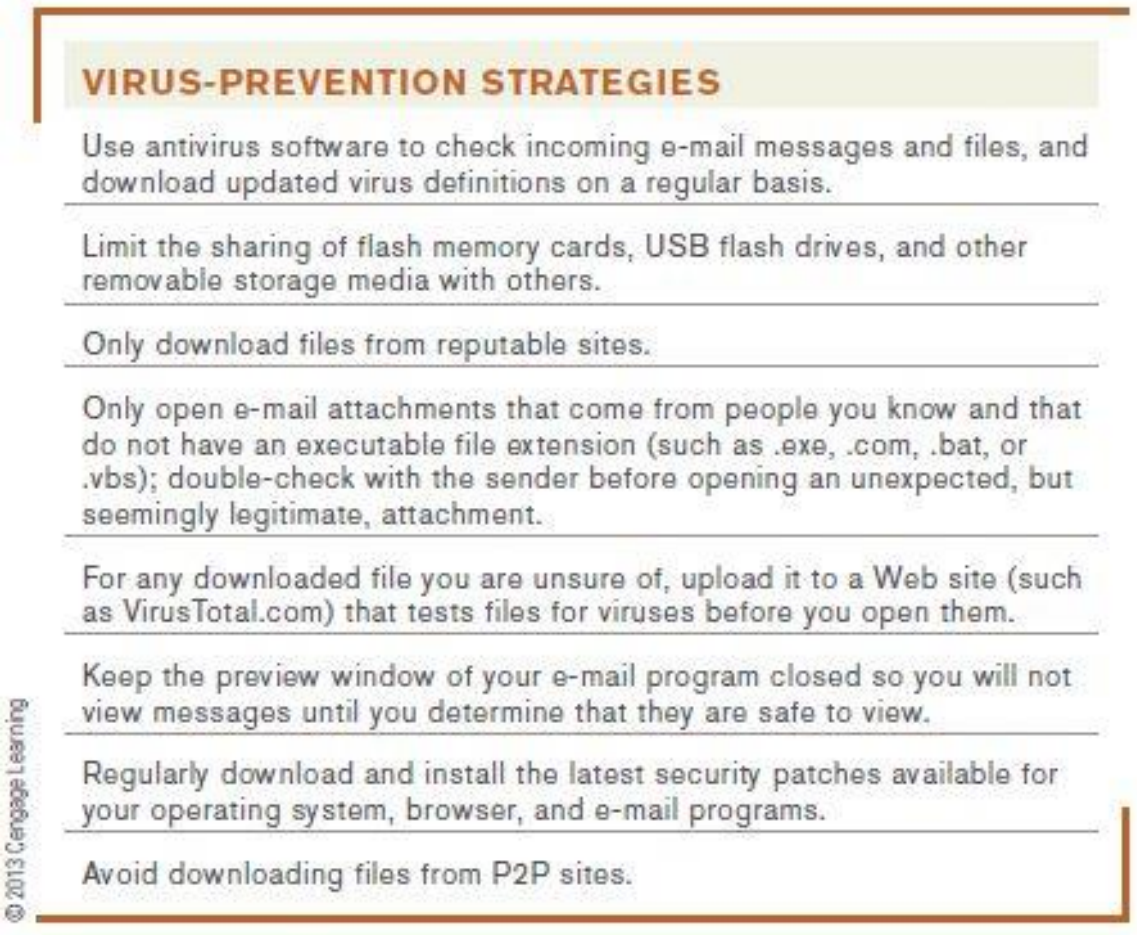


FIGURE 4-17
Security software. Most security software is set up to monitor your system on a continual basis, removing threats as they are discovered.

Protecting Against Computer Sabotage

  - Some ISPs filter include virus checking
  - E-mail authentication systems can protect against viruses sent via e-mail
- Other Security Precautions
  - Common sense precautions can help prevent a virus infection
  - Web browser security settings can help protect against some attacks

Protecting Against Computer Sabotage



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 4-18
Sensible precautions can help protect against computer virus infections.

Quick Quiz

1. Which of the following is used to control your computer by someone else?
   a. Worm
   b. Trojan horse
   c. Botnet
2. True or False: Computer viruses can only be spread via the Internet.
3. A(n) _____ is a type of malware that masquerades as something else.

Answers:

1) c; 2) False; 3) Trojan horse

Online Theft, Online Fraud, and Other Dot Cons

- Dot Con
  - A fraud or scam carried out through the Internet
  - According to the Internet Crime Complaint Center, online crime hit an all-time high in 2009
    - Slightly decreased in 2010
- Theft of Data, Information, and Other Resources
  - Data or Information Theft
    - Theft of data or information located on or being sent from a computer
    - Can occur in several ways
      - Stealing an actual computer or mobile device
      - A hacker gaining unauthorized access

Online Theft, Online Fraud, and Other Dot Cons

  - Includes personal data, proprietary corporate information, and money
- Identity Theft, Phishing, and Pharming
  - Identify Theft
    - Using someone else's identity to purchase goods or services, obtain new credit cards or bank loans, or illegally masquerade as that individual
    - Information obtained via documents, phishing schemes, stolen information, etc.
    - Expensive and time consuming to recover from
    - Identity Theft and Assumption Deterrence Act of 1998 made identity theft illegal

Online Theft, Online Fraud, and Other Dot Cons

FIGURE 4-19
How identity theft works.

© 2013 Cengage Learning

1. The thief obtains information about an individual from discarded mail, employee records, credit card transactions, Web server files, or some other method.

© Ryan McVay/Getty Images

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.

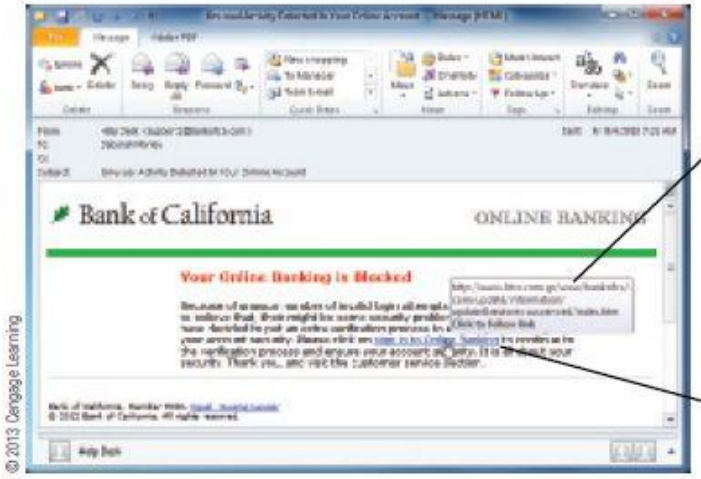
© 2013 Cengage Learning

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.

Online Theft, Online Fraud, and Other Dot Cons

- Phishing and Spear Phishing
  - Use of spoofed e-mail messages to gain credit card numbers and other personal data
  - Typically contains a link to a spoofed Web site
    - E-mails and Web sites often look legitimate
  - After victim clicks a link in the message and supplies sensitive data, that data is sent to the thief

FIGURE 4-20
Phishing. Phishing schemes use legitimate-looking e-mails to trick users into providing private information.



Online Theft, Online Fraud, and Other Dot Cons

- Spear Phishing
  - A personalized phishing scheme targeted to specific individuals
  - Often include personalized information to seem more legitimate
  - May impersonate someone in your organization, such as from the Human Resources or IT department
- Pharming
  - The use of spoofed domain names to obtain personal information
  - DNS servers are hacked to route requests for legitimate Web pages to spoofed Web pages (DNS poisoning)
  - Often take place via company DNS servers

Online Theft, Online Fraud, and Other Dot Cons

  - Drive-by Pharming
    - Hacker changes the DNS server used by a victim's router to use hacker's DNS server
- Online Auction Fraud
  - Occurs when an item purchased through an online auction is never delivered or the item is not as specified by the seller
  - It is illegal but as with other types of online fraud, prosecution is difficult

Online Theft, Online Fraud, and Other Dot Cons

- Other Internet Scams
  - A wide range of scams offered through Web sites or unsolicited e-mails
    - Loan and pyramid scams
    - Work-at-home cons
    - Soliciting of donations after disasters
    - Pornographic sites
    - Fake job site postings

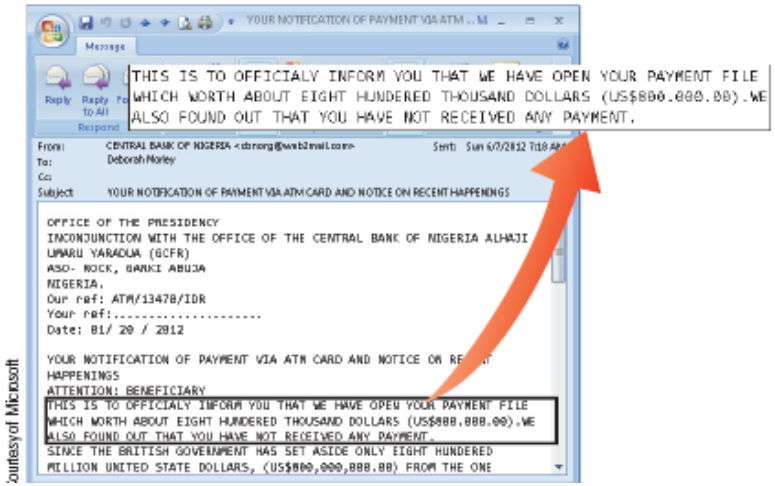


FIGURE 4-21
A Nigerian letter fraud e-mail.

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

- Protecting Against Data and Information Theft
  - Businesses should use good security measures
  - Individuals should not give out personal information (Social Security number, mother's maiden name, etc.) unless absolutely necessary
- Protecting Against Identity Theft, Phishing, and Pharming
  - Never give out sensitive information over the phone or by e-mail
  - Shred documents containing sensitive data, credit card offers, etc.
  - Don't place sensitive outgoing mail in your mailbox

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

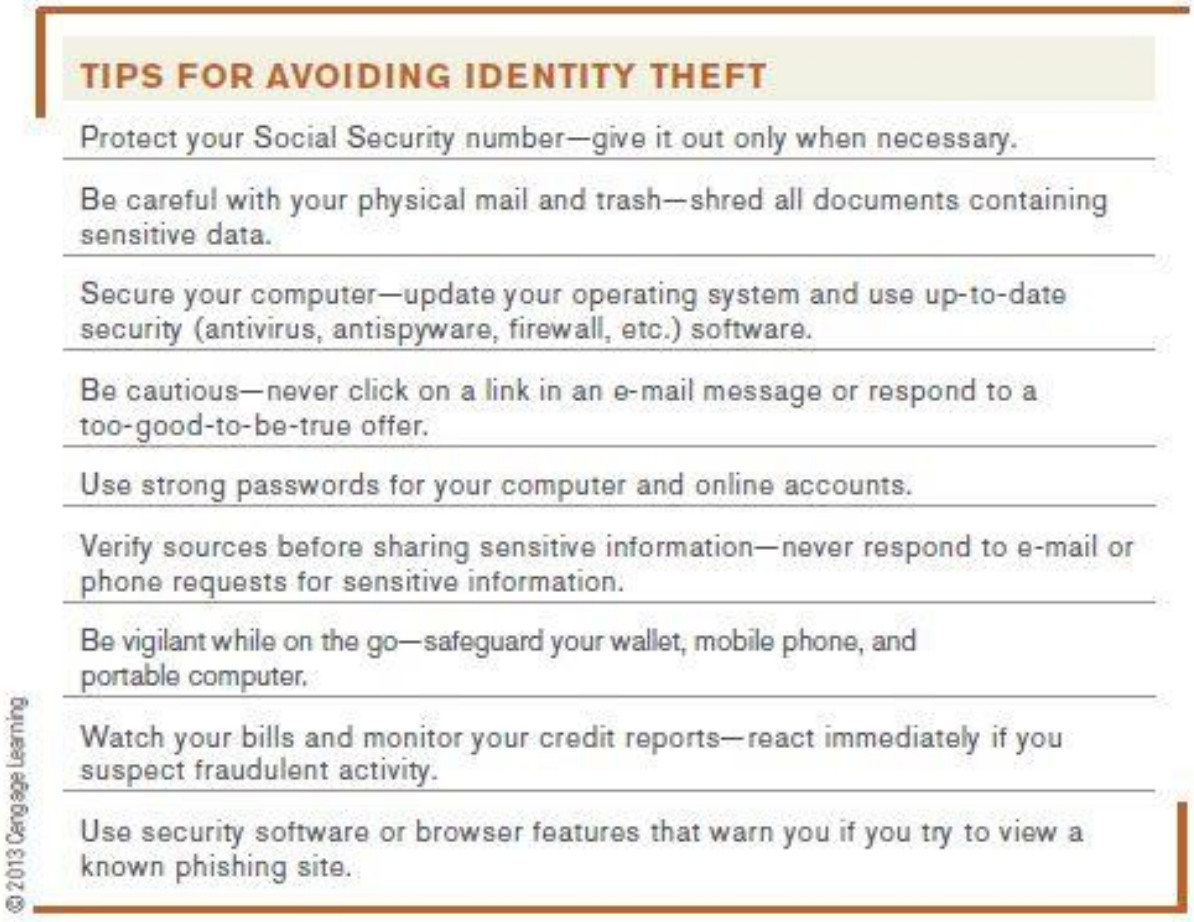
- Watch bills and credit report to detect identity theft early
- Never click a link in an e-mail message to go to a secure Web site—always type the URL in the browser instead
- Request a free credit report from 3 major consumer credit bureaus each year
- Antiphishing Tools
  - Antiphishing tools built into Web browsers can help warn you of potential phishing sites
  - Some secure sites use additional layers of security to protect against identity thieves

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

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.

FIGURE 4-22
Tips for identifying phishing e-mail messages.

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



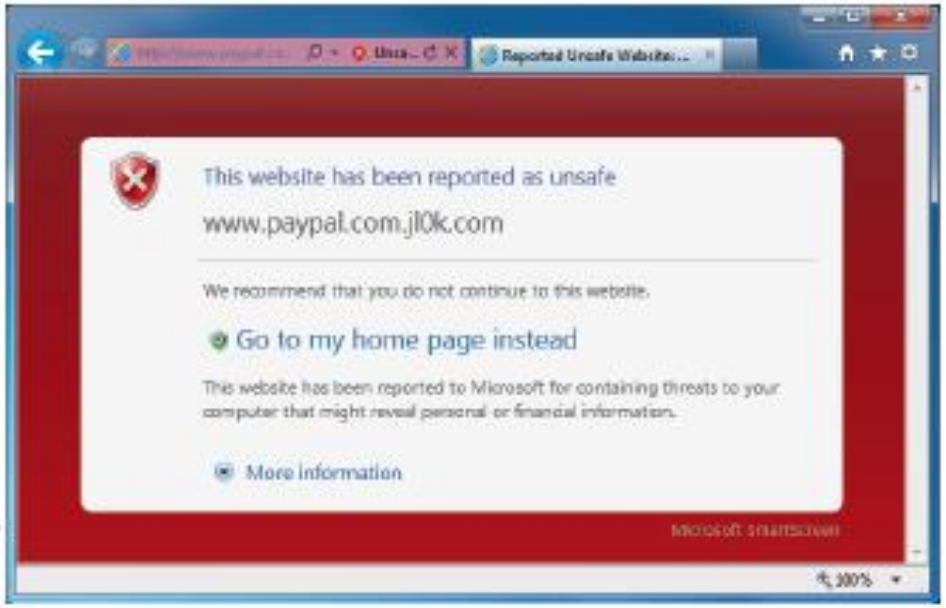
TIPS FOR AVOIDING IDENTITY THEFT

- 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 4-23
Tips to reduce your risk of identity theft.

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

- Some banks and other financial institutions add an additional step in their logon process
  - May require user to go through an authentication process



Courtesy of Microsoft

FIGURE 4-24
Unsafe Web site alerts.

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

- Digital Certificates and Digital Signatures
  - Group of electronic data that can be used to verify the identity of a person or organization
  - Obtained from Certificate Authorities
  - Typically contains identity information about the person or organization, an expiration date, and a pair of keys to be used with encryption and digital signatures
  - Are also used with secure Web sites to guarantee that the site is secure and actually belongs to the stated individual or organization
    - Can be SSL or EV SSL

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

- Digital signatures are unique digital codes that can be attached to an e-mail message or document
  - Can be used to verify the identity of the sender
  - Can be used to guarantee the message or file has not been changed since it was signed
  - Uses public key encryption
    - Document is signed with the sender's private key
    - The key and the document create a unique digital signature
    - Signature is verified using the sender's public key

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

FIGURE 4-25
EV SSL certificates.
The browser's Address bar reflects information about the digital certificate being used.

Courtesy of Microsoft

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

- Protecting Against Online Auction Fraud and Other Internet Scams
  - Use common sense
  - Check online auction seller's feedback before bidding
  - Pay for online purchases via a credit card so transactions can be disputed if needed
  - Use an online payment system
  - Take advantage of buyer protection
  - Use an escrow service for high-priced items

Personal Safety Issues

- Cyberbullying and Cyberstalking
  - Cyberbullying
    - Children or teenagers bullying other children or teenagers via the Internet
      - E-mails
      - Social networking sites
      - Blogs
    - Common today--estimated to affect 50% of all US teenagers

Personal Safety Issues

- Cyberstalking
  - Repeated threats or harassing behavior between adults carried out via e-mail or another Internet communication method
    - Sending harassing e-mail messages to the victim
    - Sending unwanted files to the victim
    - Posting inappropriate messages about the victim
    - Signing the victim up for offensive material
    - Publicizing the victim's contact information
    - Hacking into victim's social networking pages
  - Sometimes escalates to personal violence

Personal Safety Issues

- Online Pornography
  - Concern for parents and schools
  - Difficult to stop due to constitutional rights
  - Online pornography involving minors is illegal
  - Link between online pornography and child molestation
  - Internet can make it easier to arrange dangerous meetings between predators and children

Protecting Against Cyberbullying, Cyberstalking, and Other Personal Safety Concerns

- Safety Tips for Adults
  - Be cautious and discreet online
  - Use gender-neutral, nonprovocative identifying names
  - Do not reveal personal information
  - Do not respond to any insults or other harassing comments
  - Can request your personal information be removed from online directories

Protecting Against Cyberbullying, Cyberstalking, and Other Personal Safety Concerns

- Safety Tips for Children and Teens
  - Parents should monitor their children's computer and smart phone activities
  - Children and teenagers should be told what activities are allowed
  - Personal information should never be revealed online
  - Instruct children and teens to tell parents, or a teacher if at school, if someone ever requests personal information, a personal meeting, or threatens or harasses them
  - Older children should be cautioned about posting and/or sending compromising photographs or sexually explicit messages (sexting)

Quick Quiz

1. Sending an e-mail that looks like it came from someone else in order to obtain information for fraudulent purposes is called _____.
   a. hacking
   b. online auction fraud
   c. phishing
2. True or False: Cyberstalkers often find their victims online.
3. Using someone else's identity to purchase goods or services or perform other transactions is called _____.

Answers:

1) c; 2) True; 3) identity theft

Summary

- Why Be Concerned About Network and Internet Security?
- Unauthorized Access and Unauthorized Use
- Protecting Against Unauthorized Access and Unauthorized Use
- Computer Sabotage
- Protecting Against Computer Sabotage
- Online Theft, Online Fraud, and Other Dot Cons
- Protecting Against Online Theft, Online Fraud, and Other Dot Cons
- Personal Safety Issues