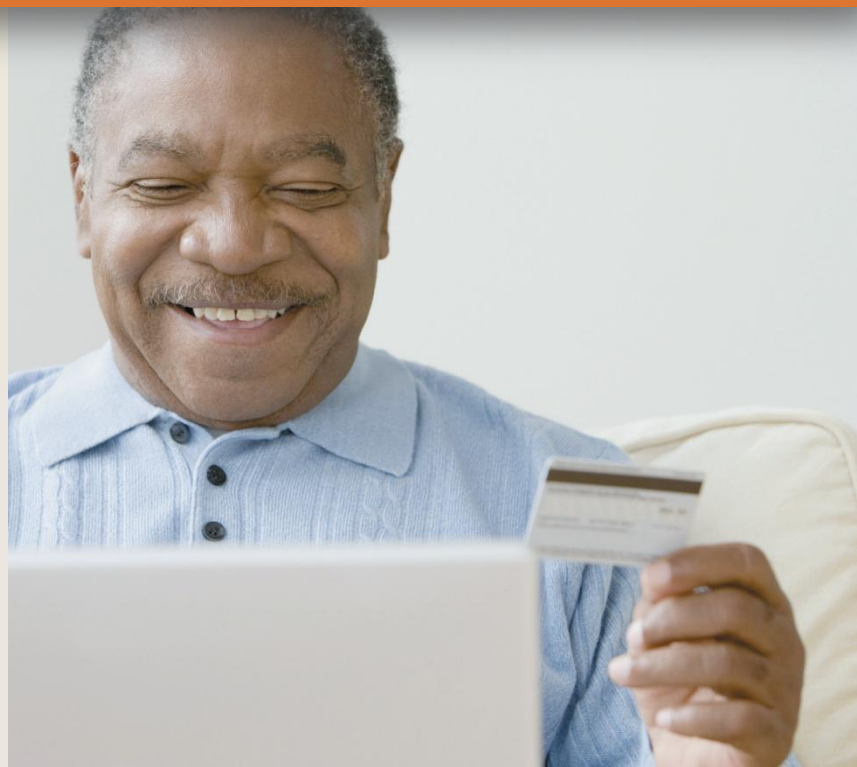
Chapter Eleven

Computer Security and Safety, Ethics, and Privacy

Discovering Computers 2012

Your Interactive Guide to the Digital World



Objectives Overview

Define the term, computer security risks, and briefly describe the types of cybercrime perpetrators

Describe various types of Internet and network attacks, and identify ways to safeguard against these attacks

Discuss techniques to prevent unauthorized computer access and use

Identify safeguards against hardware theft and vandalism

Explain the ways software manufacturers protect against software piracy

Discuss how encryption works, and explain why it is necessary

See Page 555
for Detailed Objectives

Objectives Overview

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

Explain the options available for backing up computer resources

Identify risks and safeguards associated with wireless communications

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

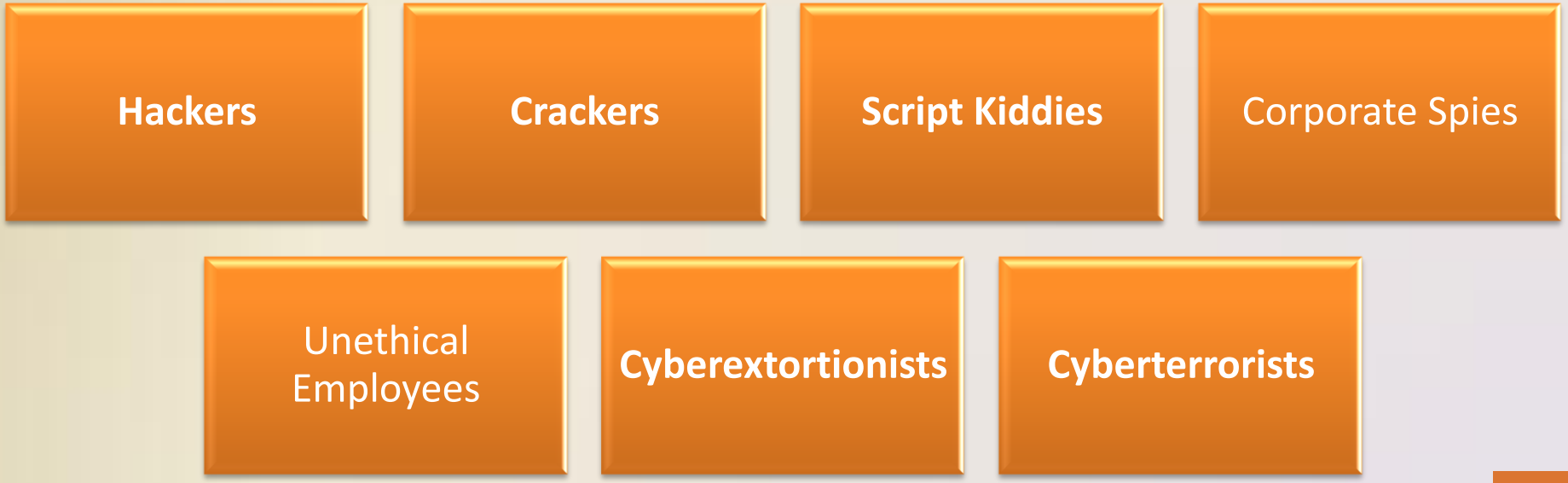
Recognize issues related to information accuracy, intellectual property rights, codes of conduct, and green computing

Discuss issues surrounding information privacy

See Page 555
for Detailed Objectives

Computer Security Risks

- A **computer security risk** is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability
- A **cybercrime** is an online or Internet-based illegal act



Computer Security Risks

Pages 556 – 557
Figure 11-1

Internet and Network Attacks

- Information transmitted over networks has a higher degree of security risk than information kept on an organization's premises
- An **online security service** is a Web site that evaluates your computer to check for Internet and e-mail vulnerabilities

Popular Online Security Services for Personal Computers

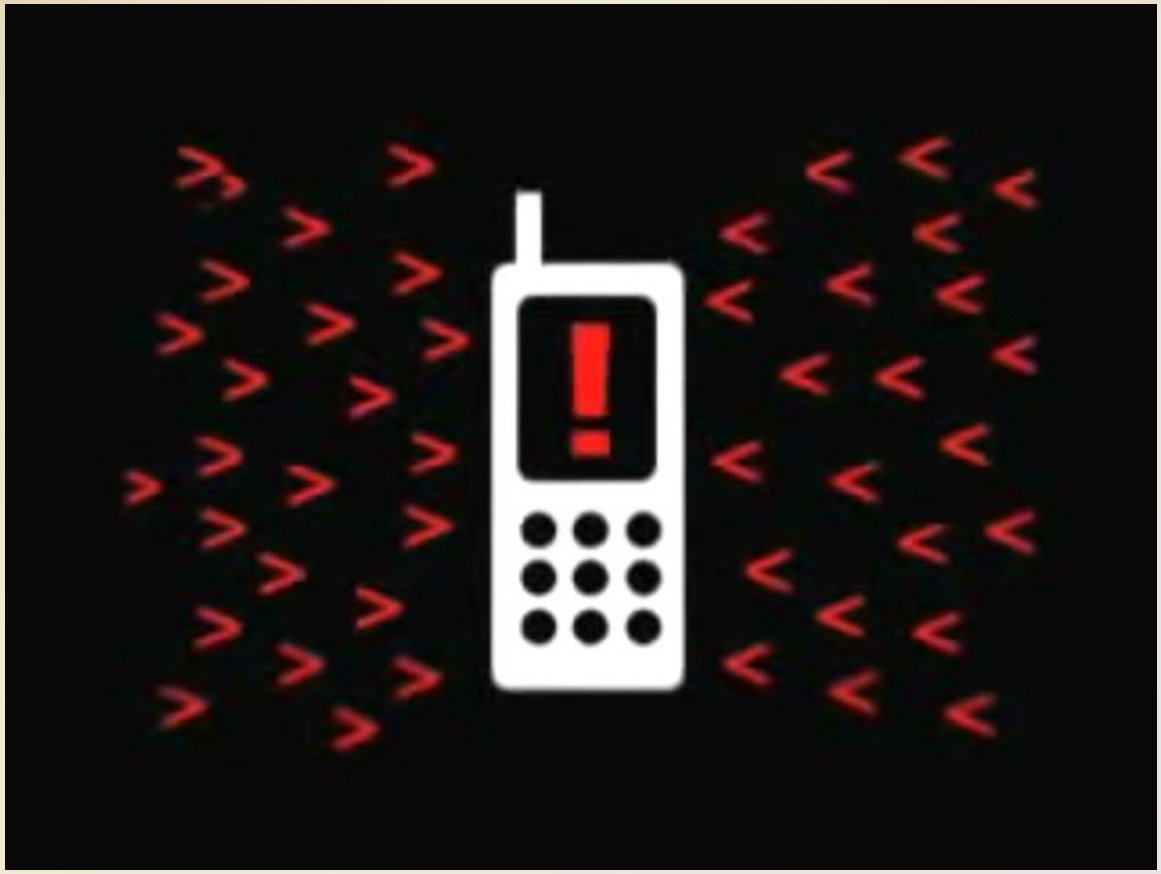
Name of Online Service	Web Address
Audit My PC	http://www.auditmypc.com/firewall-test.asp
McAfee FreeScan	http://home.mcafee.com/Downloads/FreeScan.aspx
Symantec Security Check	http://security.symantec.com/sscv6/home.asp
Trend Micro House Call	http://housecall.trendmicro.com/

Page 558
Figure 11-2

Internet and Network Attacks

Computer **Virus**	**Worm**	**Trojan Horse**	**Rootkit**
• Affects a computer negatively by altering the way the computer works	• Copies itself repeatedly, using up resources and possibly shutting down the computer or network	• A malicious program that hides within or looks like a legitimate program	• Program that hides in a computer and allows someone from a remote location to take full control

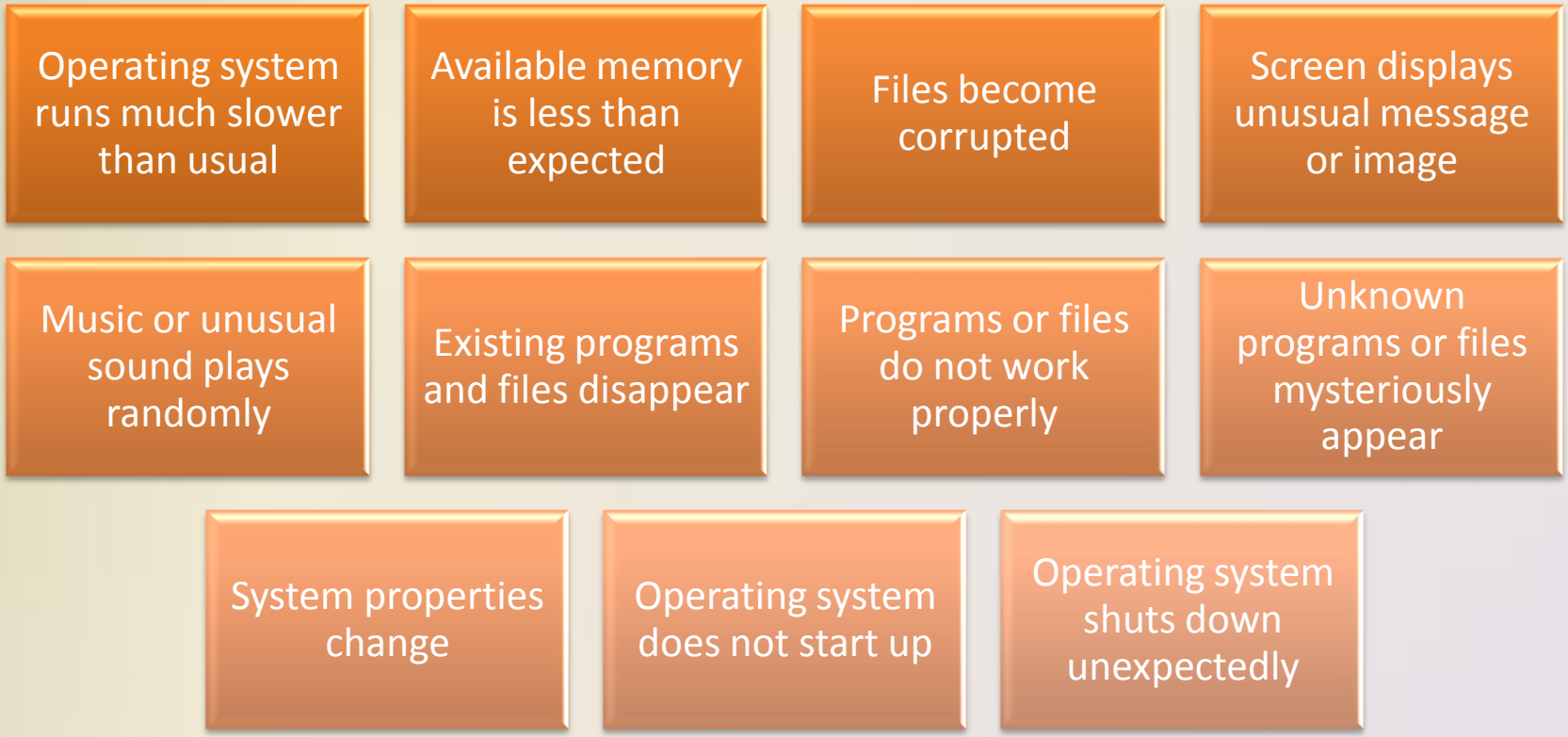
Video: Attack of the Mobile Viruses



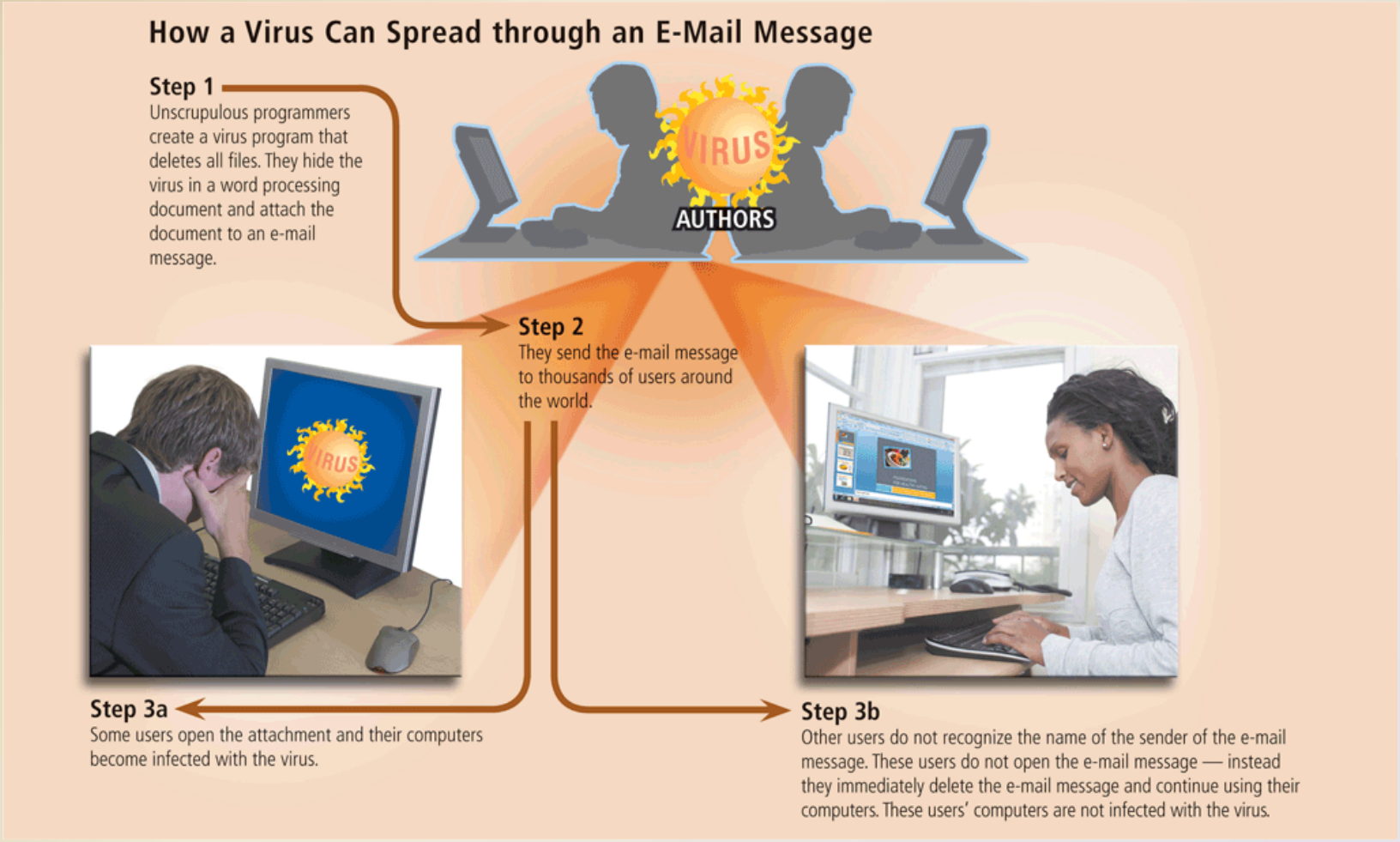
CLICK TO START

Internet and Network Attacks

- An infected computer has one or more of the following symptoms:

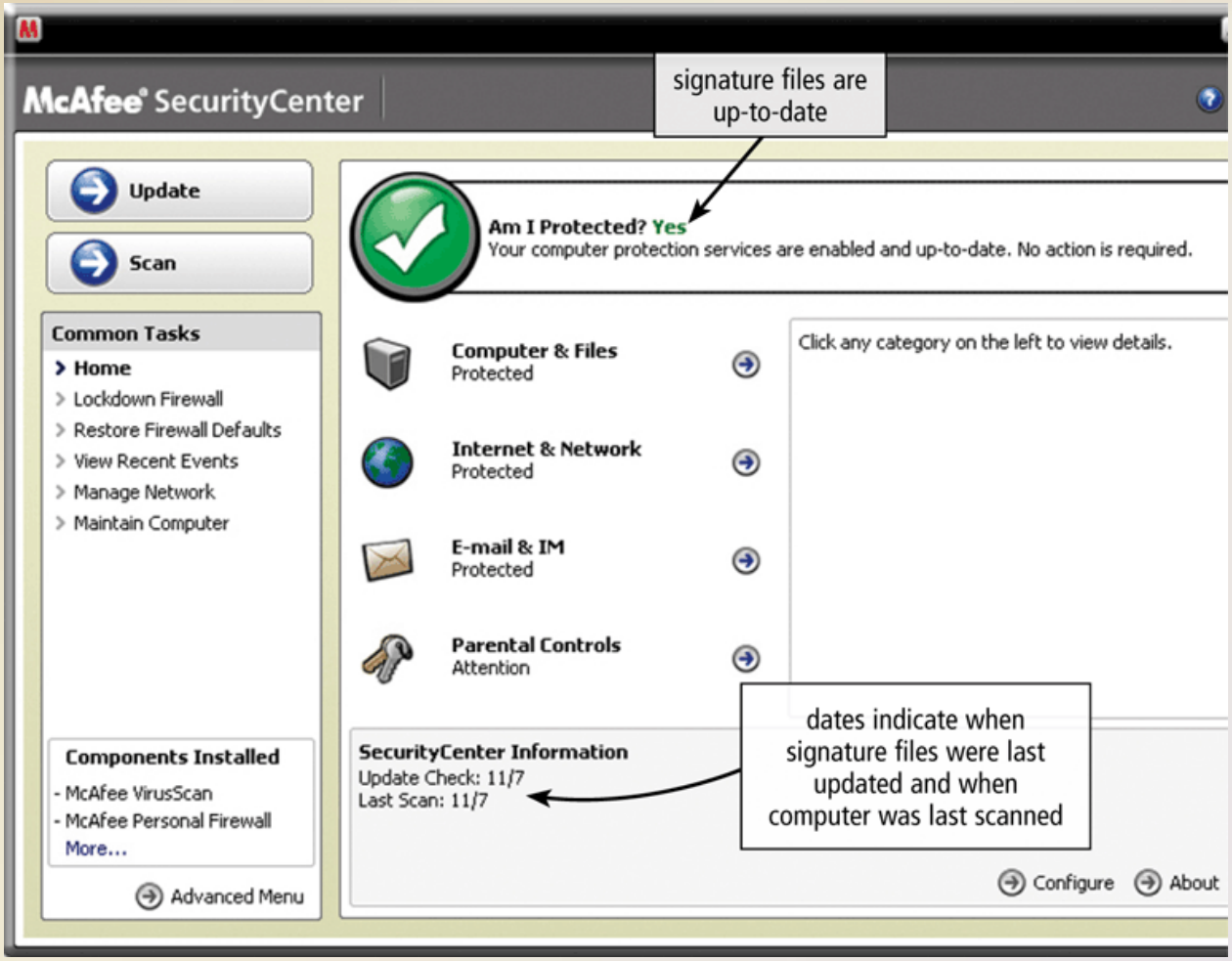


Internet and Network Attacks



Page 559
Figure 11-3

Internet and Network Attacks



Internet and Network Attacks

- Users can take several precautions to protect their home and work computers and mobile devices from these malicious infections

Tips for Preventing Viruses and Other Malware

1. Never start a computer with removable media inserted in the drives or plugged in the ports, unless the media are uninfected.
2. Never open an e-mail attachment unless you are expecting it *and* it is from a trusted source.
3. Set the macro security in programs so that you can enable or disable macros. Enable macros only if the document is from a trusted source and you are expecting it.
4. Install an antivirus program on all of your computers. Update the software and the virus signature files regularly.
5. Scan all downloaded programs for viruses and other malware.
6. If the antivirus program flags an e-mail attachment as infected, delete or quarantine the attachment immediately.
7. Before using any removable media, scan the media for malware. Follow this procedure even for shrink-wrapped software from major developers. Some commercial software has been infected and distributed to unsuspecting users.
8. Install a personal firewall program.
9. Stay informed about new virus alerts and virus hoaxes.

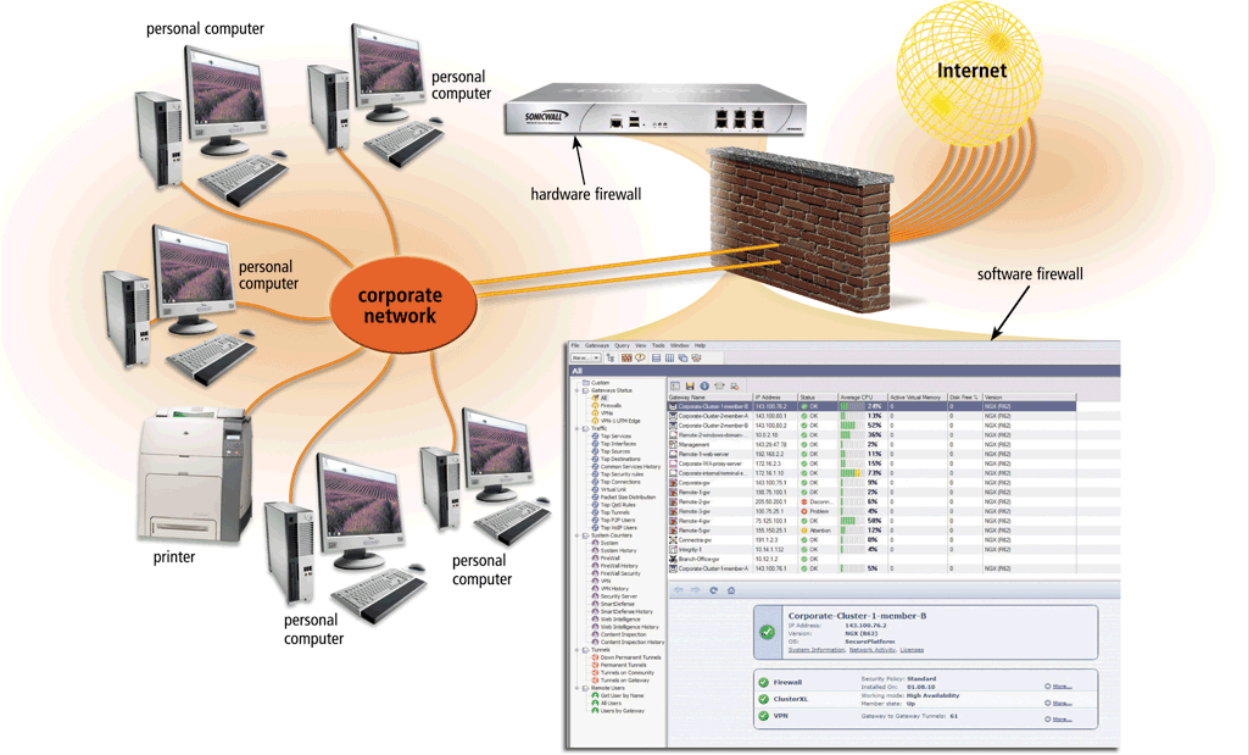
Page 560 – 561
Figure 11-7

Internet and Network Attacks

- A **botnet** is a group of compromised computers connected to a network
  - A compromised computer is known as a **zombie**
- A **denial of service attack** (**DoS attack**) disrupts computer access to Internet services
  - Distributed DoS (DDoS)
- A **back door** is a program or set of instructions in a program that allow users to bypass security controls
- **Spoofing** is a technique intruders use to make their network or Internet transmission appear legitimate

Internet and Network Attacks

- A **firewall** is hardware and/or software that protects a network's resources from intrusion



Pages 563 - 564
Figure 11-8

Internet and Network Attacks

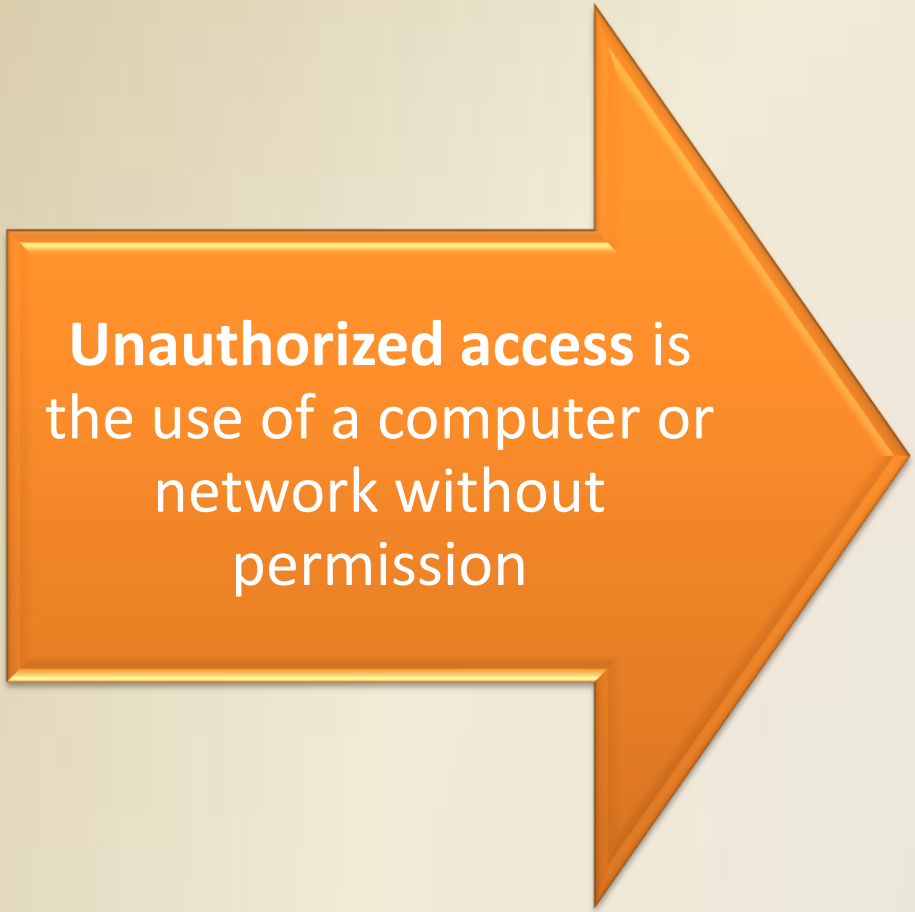
Intrusion detection software

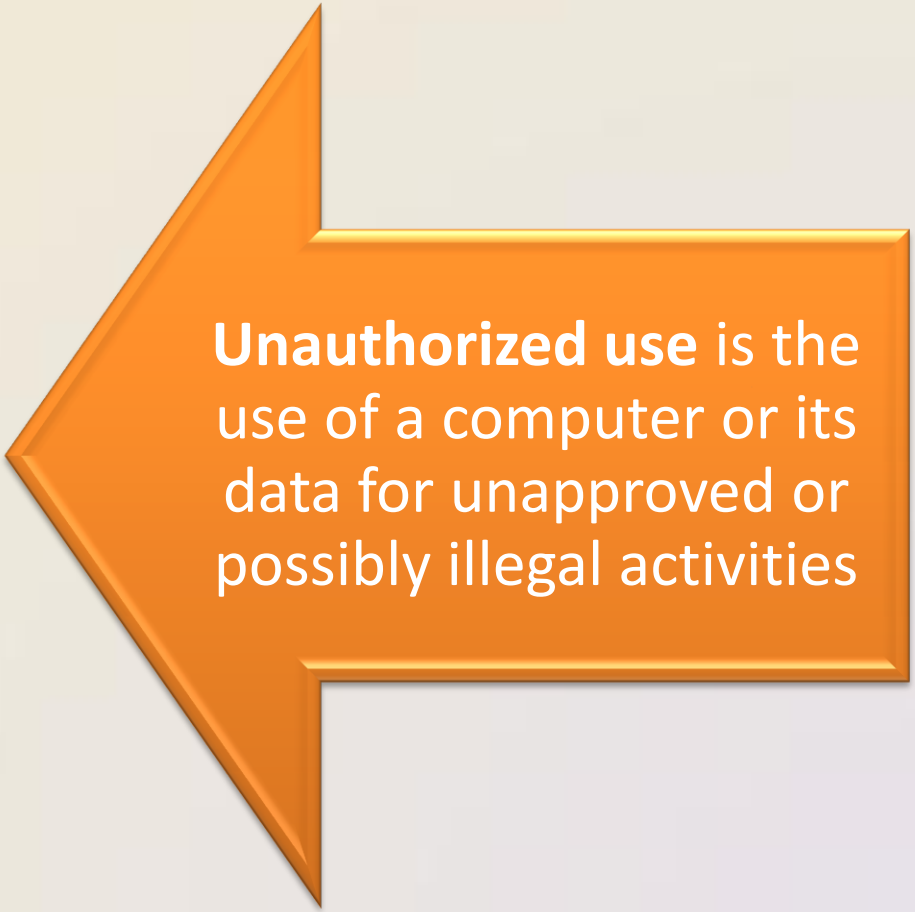
- Analyzes all network traffic
- Assesses system vulnerabilities
- Identifies any unauthorized intrusions
- Notifies network administrators of suspicious behavior patterns or system breaches

Honeypot

- Vulnerable computer that is set up to entice an intruder to break into it

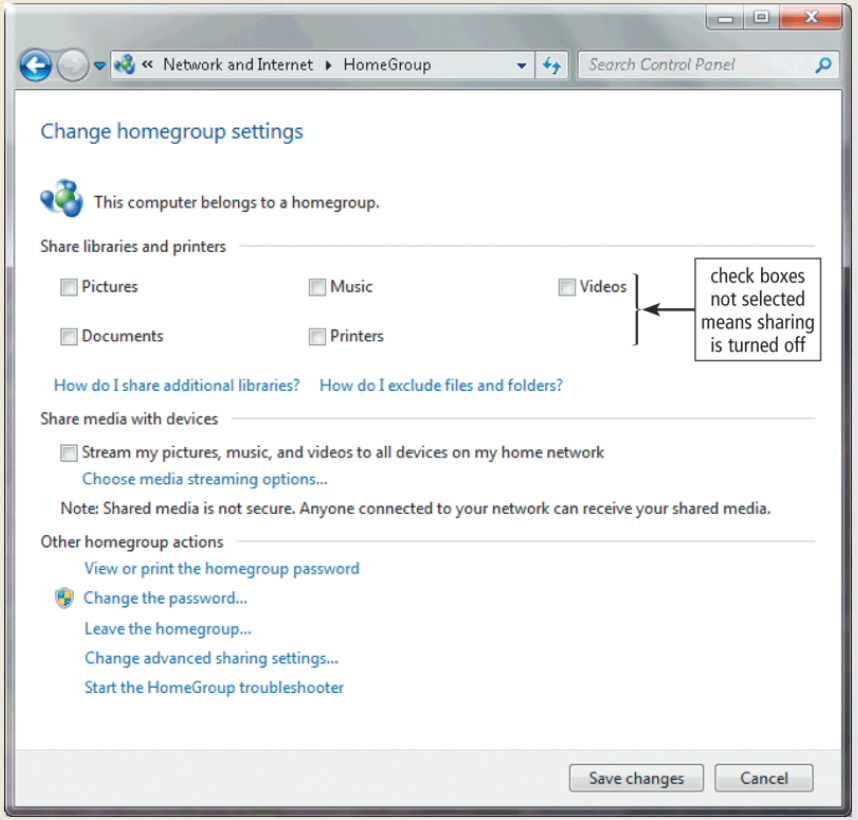
Unauthorized Access and Use





Unauthorized Access and Use

- Organizations take several measures to help prevent unauthorized access and use
  - Acceptable use policy
  - Disable file and printer sharing
  - Firewalls
  - Intrusion detection software



Unauthorized Access and Use

- Access controls define who can access a computer, when they can access it, and what actions they can take
  - Two-phase processes called identification and authentication
  - **User name**
  - **Password**
  - Passphrase
  - CAPTCHA

Pages 565 – 567
Figure 11-11

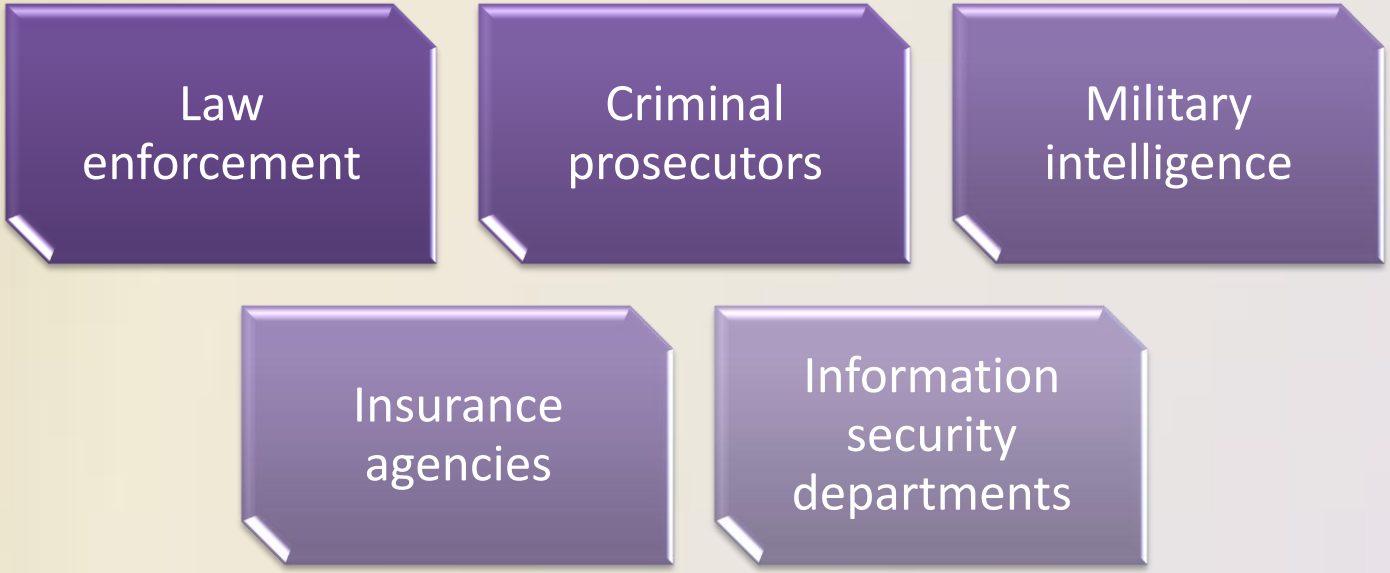
Unauthorized Access and Use

- A possessed object is any item that you must carry to gain access to a computer or computer facility
  - Often are used in combination with a **personal identification number** (**PIN**)
- A **biometric device** authenticates a person's identity by translating a personal characteristic into a digital code that is compared with a digital code in a computer

Page 568
Figure 11-14

Unauthorized Access and Use

- **Digital forensics** is the discovery, collection, and analysis of evidence found on computers and networks
- Many areas use digital forensics



Hardware Theft and Vandalism

Hardware theft is the act of stealing computer equipment

Hardware vandalism is the act of defacing or destroying computer equipment

Hardware Theft and Vandalism

- To help reduce the of chances of theft, companies and schools use a variety of security measures

Physical access controls

Alarm systems

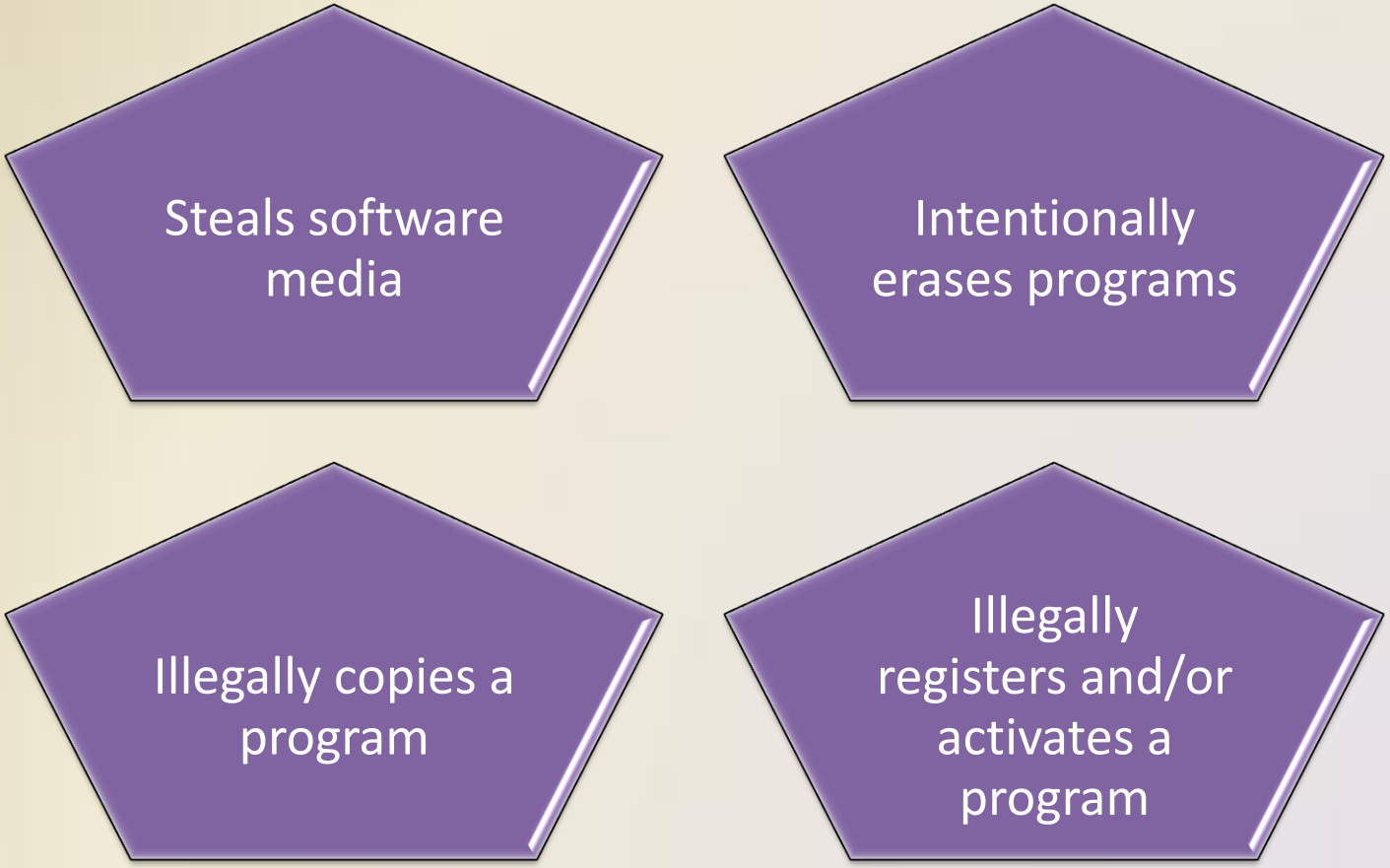
Cables to lock equipment

Real time location system

Passwords, possessed objects, and biometrics

Software Theft

- **Software theft** occurs when someone:



Software Theft

- A single-user **license agreement** typically contains the following conditions:

Permitted to

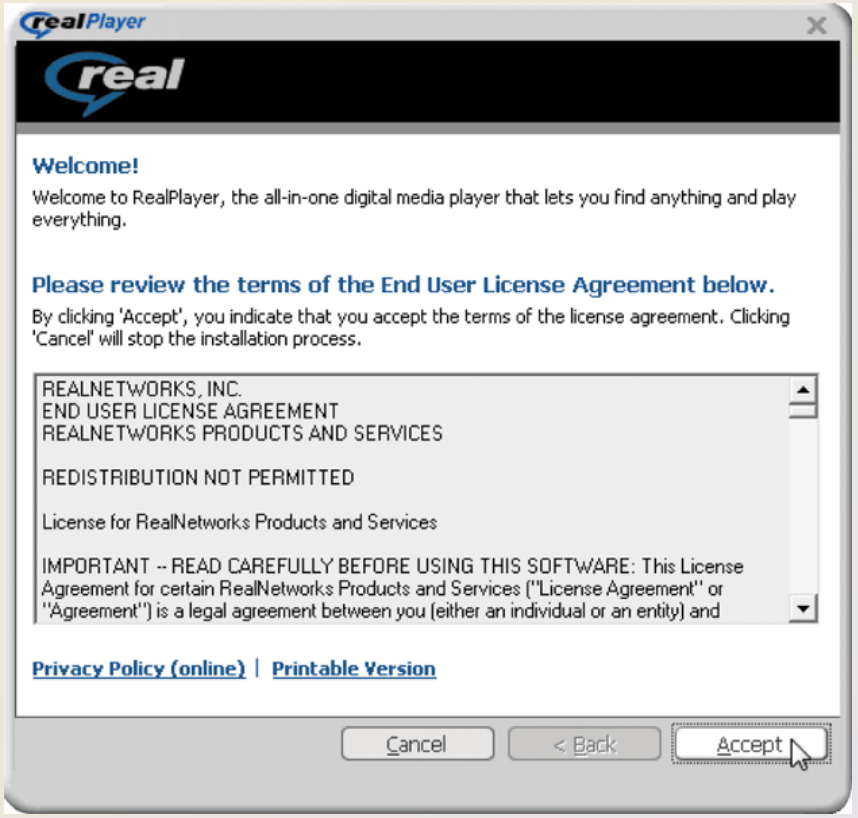
- Install the software on one computer
- Make one copy of the software
- Remove the software from your computer before giving it away or selling it

Not permitted to

- Install the software on a network
- Give copies to friends or colleagues while continuing to use the software
- Export the software
- Rent or lease the software

Software Theft

- Copying, loaning, borrowing, renting, or distributing software can be a violation of copyright law
- Some software requires **product activation** to function fully



Information Theft

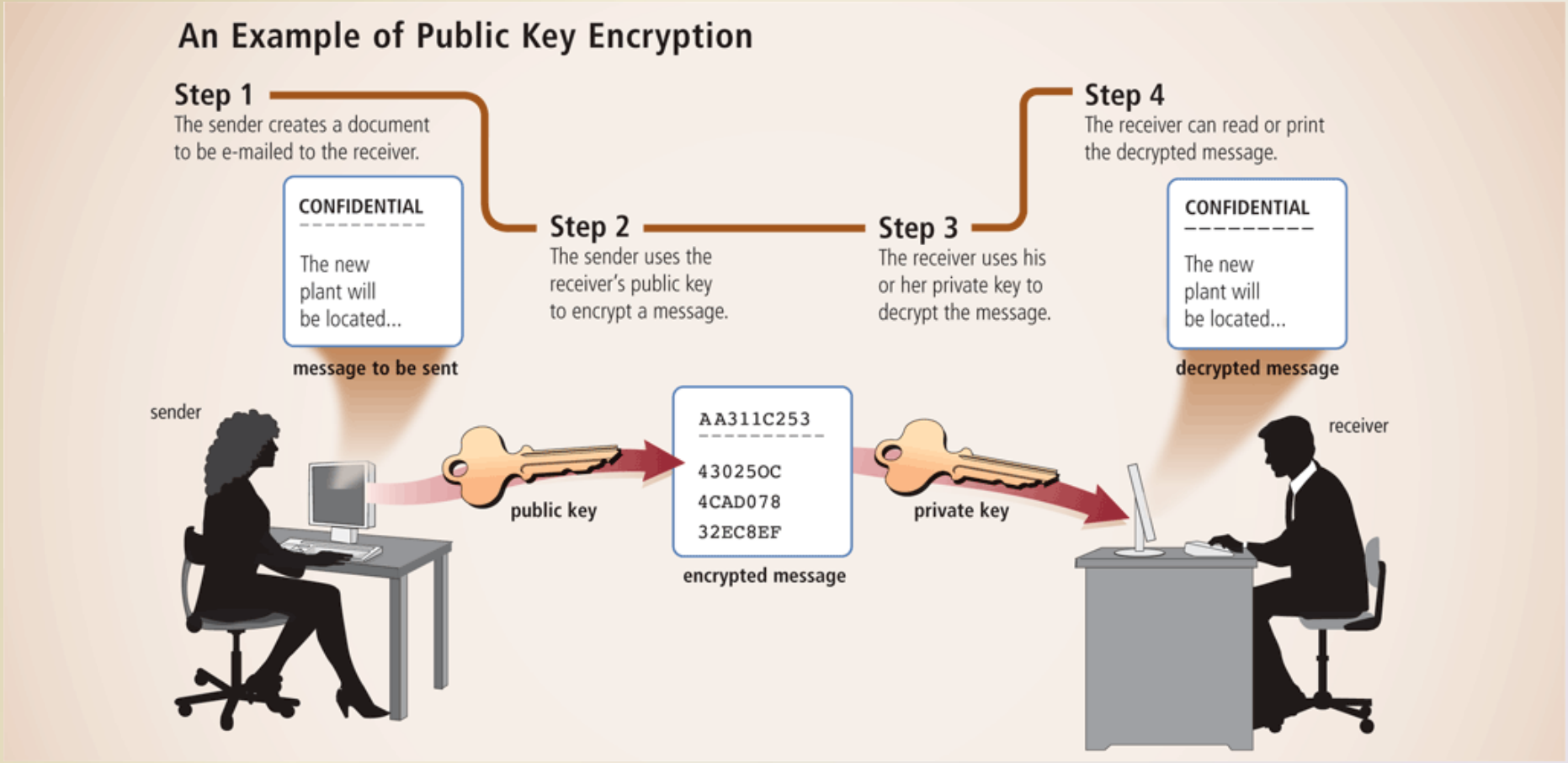
- **Information theft** occurs when someone steals personal or confidential information
- **Encryption** is a process of converting readable data into unreadable characters to prevent unauthorized access

Simple Encryption Algorithms

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

Pages 572 - 573
Figure 11-17

Information Theft



Page 573
Figure 11-18

Information Theft

- A **digital signature** is an encrypted code that a person, Web site, or organization attaches to an electronic message to verify the identity of the sender
  - Often used to ensure that an impostor is not participating in an Internet transaction
- Web browsers and Web sites use encryption techniques

Information Theft

- Popular security techniques include

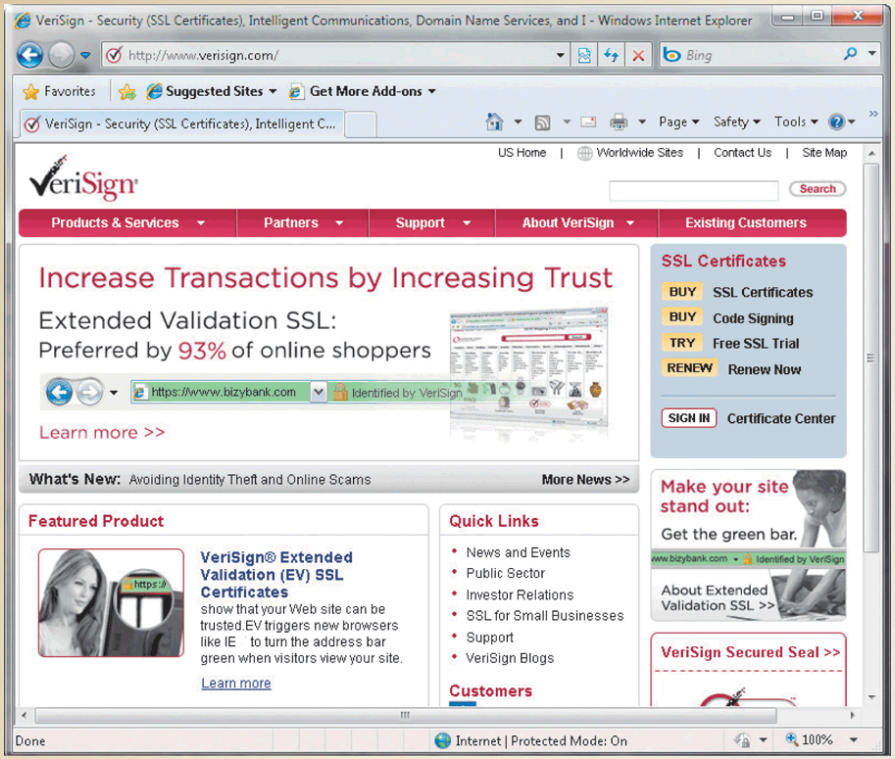
Digital Certificates

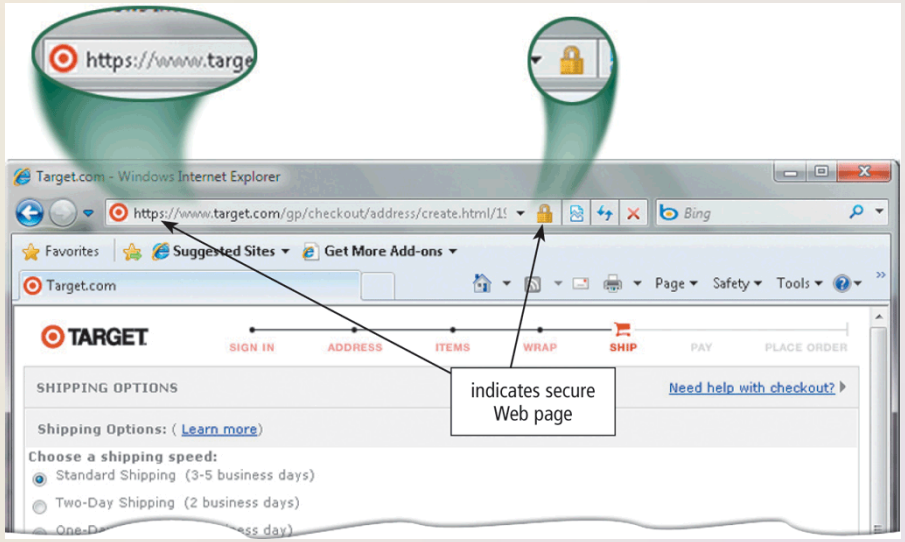
Transport Layer Security (TLS)

Secure HTTP

VPN

Information Theft





Pages 574 - 575
Figures 11-19 – 11-20

System Failure

- A system failure is the prolonged malfunction of a computer
- A variety of factors can lead to system failure, including:
  - Aging hardware
  - Natural disasters
  - Electrical power problems
    - **Noise**, **undervoltages**, and **overvoltages**
  - Errors in computer programs

System Failure

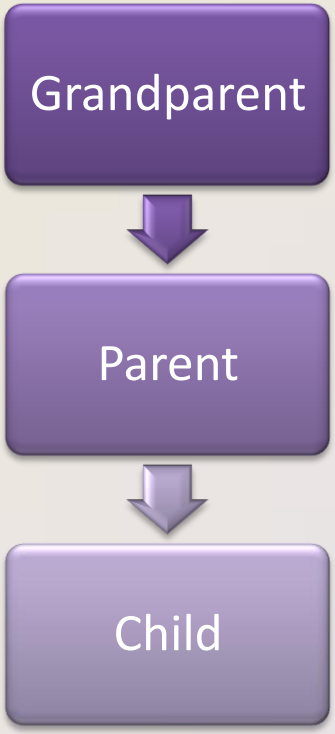
- Two ways to protect from system failures caused by electrical power variations include **surge protectors** and **uninterruptable power supplies** (**UPS**)

Backing Up – The Ultimate Safeguard

- A **backup** is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed
  - To **back up** a file means to make a copy of it
- Offsite backups are stored in a location separate from the computer site

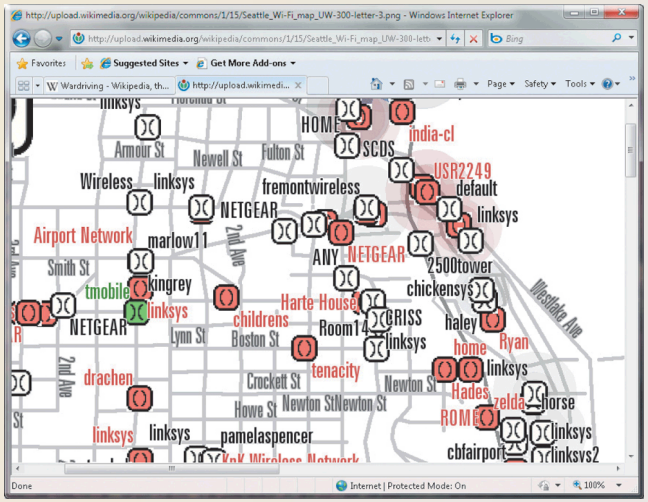
Backing Up – The Ultimate Safeguard

- Two categories of backups:
  - Full backup
  - Selective backup
- Three-generation backup policy



Wireless Security

- Wireless access poses additional security risks
  - About 80 percent of wireless networks have no security protection
- War driving allows individuals to detect wireless networks while driving a vehicle through the area



Wireless Security

- In additional to using firewalls, some safeguards improve security of wireless networks:

A wireless access point should not broadcast an SSID

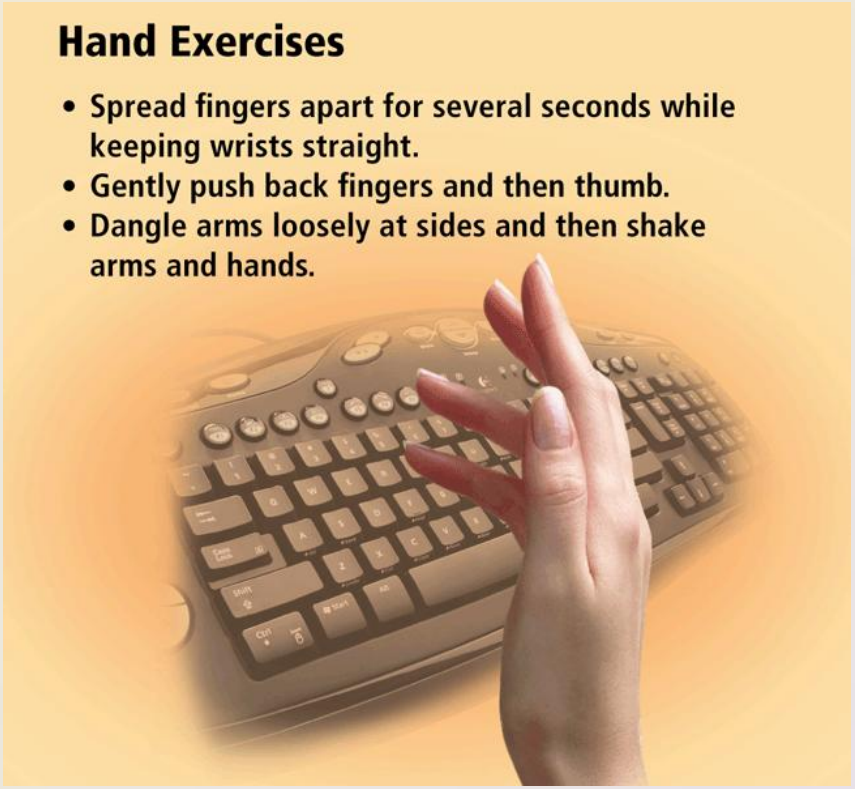
Change the default SSID

Configure a WAP so that only certain devices can access it

Use WPA or WPA2 security standards

Health Concerns of Computer Use

- The widespread use of computers has led to health concerns
  - **Repetitive strain injury (RSI)**
    - Tendonitis
    - Carpal tunnel syndrome (CTS)
  - **Computer vision syndrome** (CVS)



Page 579
Figure 11-24

Health Concerns of Computer Use

Techniques to Ease Eyestrain

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

Page 580
Figure 11-25

Health Concerns of Computer Use

- Ergonomics is an applied science devoted to incorporating comfort, efficiency, and safety into the design of items in the workplace

Health Concerns of Computer Use

- **Computer addiction** occurs when the computer consumes someone's entire social life
- Symptoms of users include:

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

Ethics and Society

- **Computer ethics** are the moral guidelines that govern the use of computers and information systems
- Information accuracy is a concern
  - Not all information on the Web is correct

Pages 581 – 582
Figure 11-28

Ethics and Society

Intellectual property rights are the rights to which creators are entitled for their work

- A **copyright** protects any tangible form of expression

An IT **code of conduct** is a written guideline that helps determine whether a specific computer action is ethical or unethical

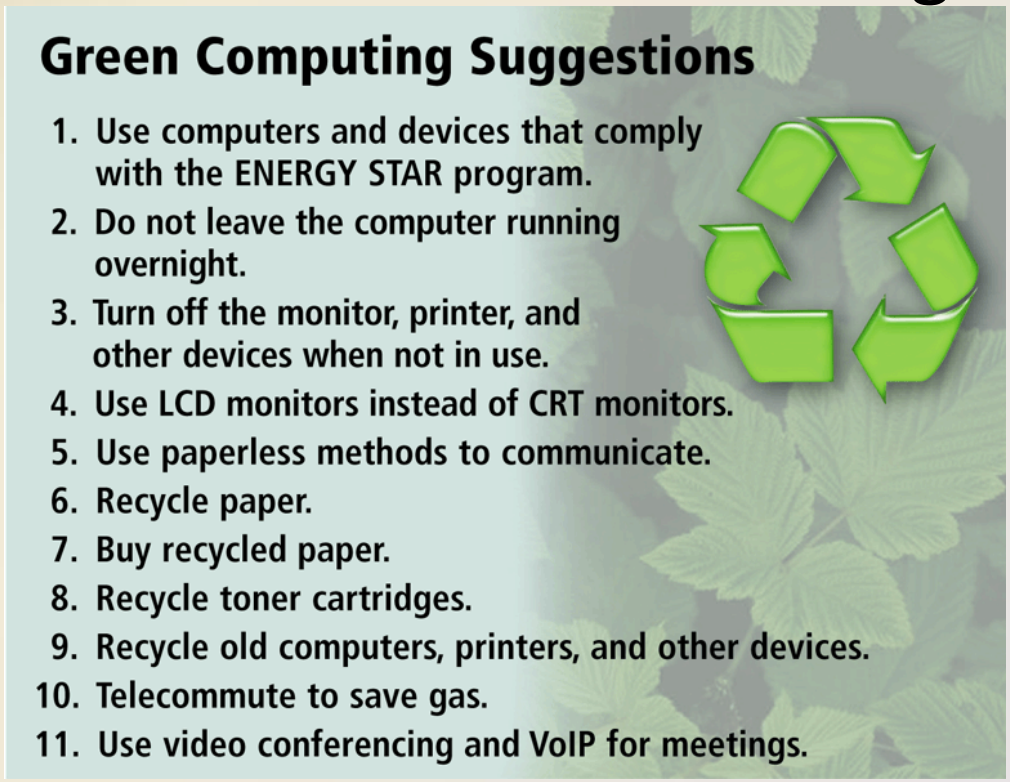
Ethics and Society

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

Page 583
Figure 11-29

Ethics and Society

- **Green computing** involves reducing the electricity and environmental waste while using a computer



Pages 583 – 584
Figure 11-30

Ethics and Society

- **Information privacy** refers to the right of individuals and companies to deny or restrict the collection and use of information about them
- Huge databases store data online
- It is important to safeguard your information

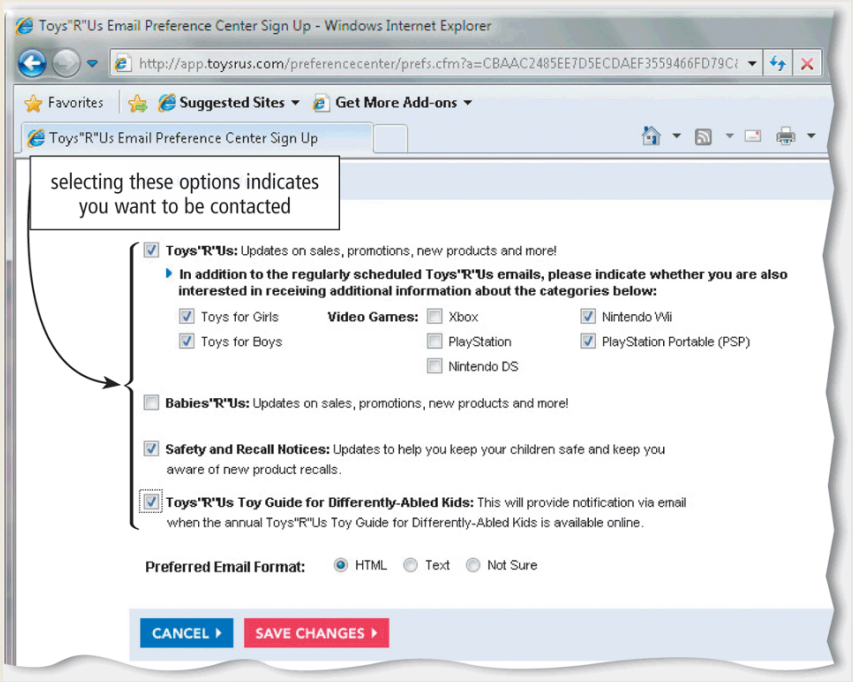
Ethics and Society

How to Safeguard Personal Information

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

Ethics and Society

- When you fill out a form, the merchant that receives the form usually enters it into a database
- Many companies today allow people to specify whether they want their personal information distributed



Ethics and Society

- A **cookie** is a small text file that a Web server stores on your computer
- Web sites use cookies for a variety of reasons:

Allow for personalization

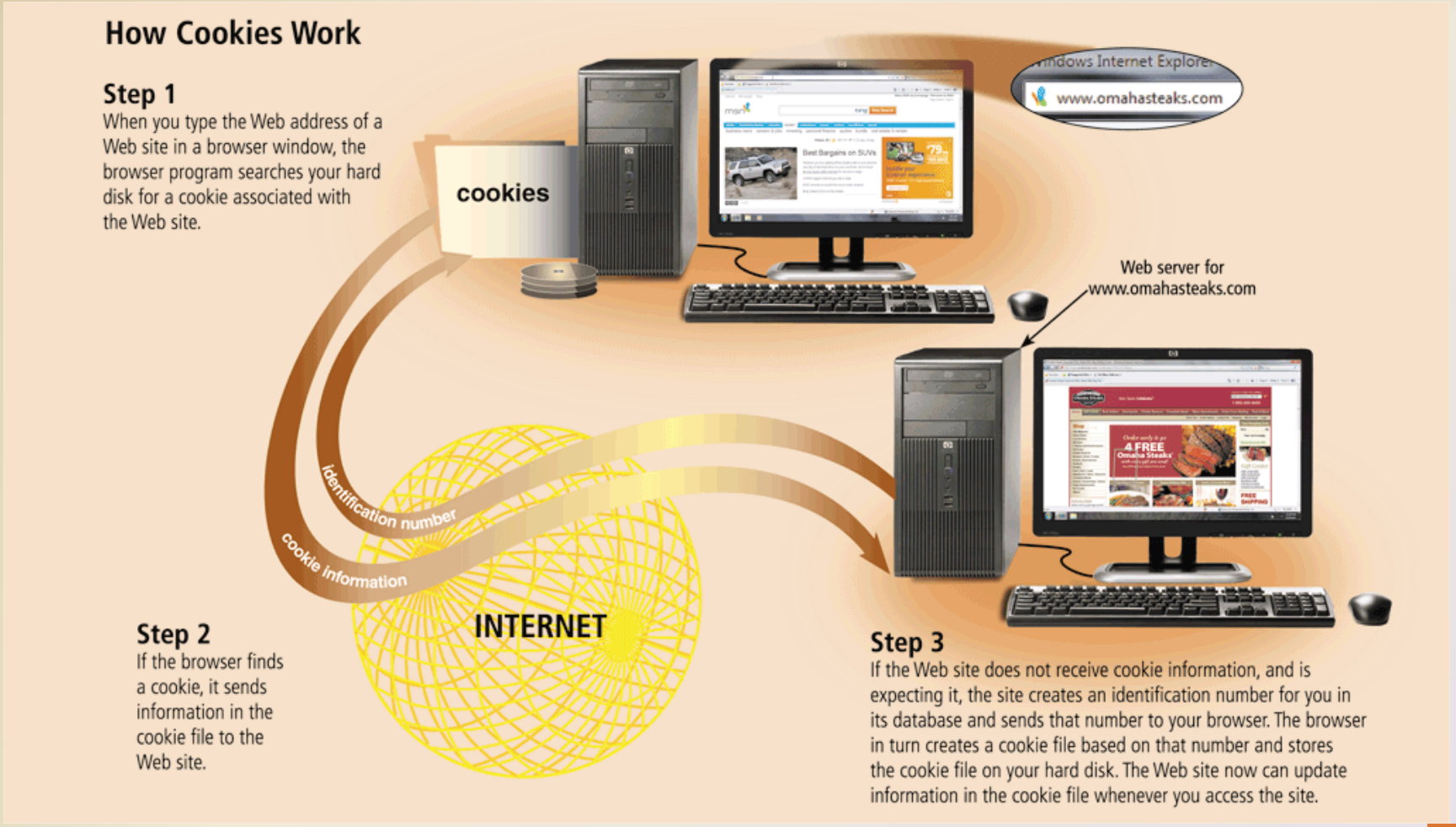
Store users' passwords

Assist with online shopping

Track how often users visit a site

Target advertisements

Ethics and Society

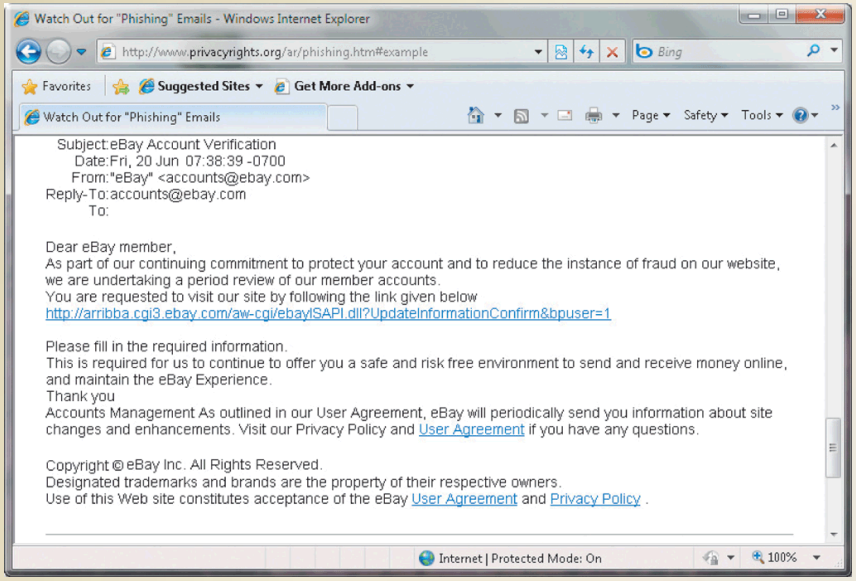


Page 586
Figure 11-33

Ethics and Society

- **Spam** is an unsolicited e-mail message or newsgroup posting
- **E-mail filtering** blocks e-mail messages from designated sources
- **Anti-spam programs** attempt to remove spam before it reaches your inbox

Ethics and Society



- **Phishing** is a scam in which a perpetrator sends an official looking e-mail message that attempts to obtain your personal and financial information
- **Pharming** is a scam where a perpetrator attempts to obtain your personal and financial information via spoofing

Pages 587 - 588
Figure 11-35

Ethics and Society

- The concern about privacy has led to the enactment of federal and state laws regarding the storage and disclosure of personal data
  - See Figure 11-36 on page 589 for a listing of major U.S. government laws concerning privacy
- The 1970 **Fair Credit Reporting Act** limits the rights of others viewing a credit report to only those with a legitimate business need

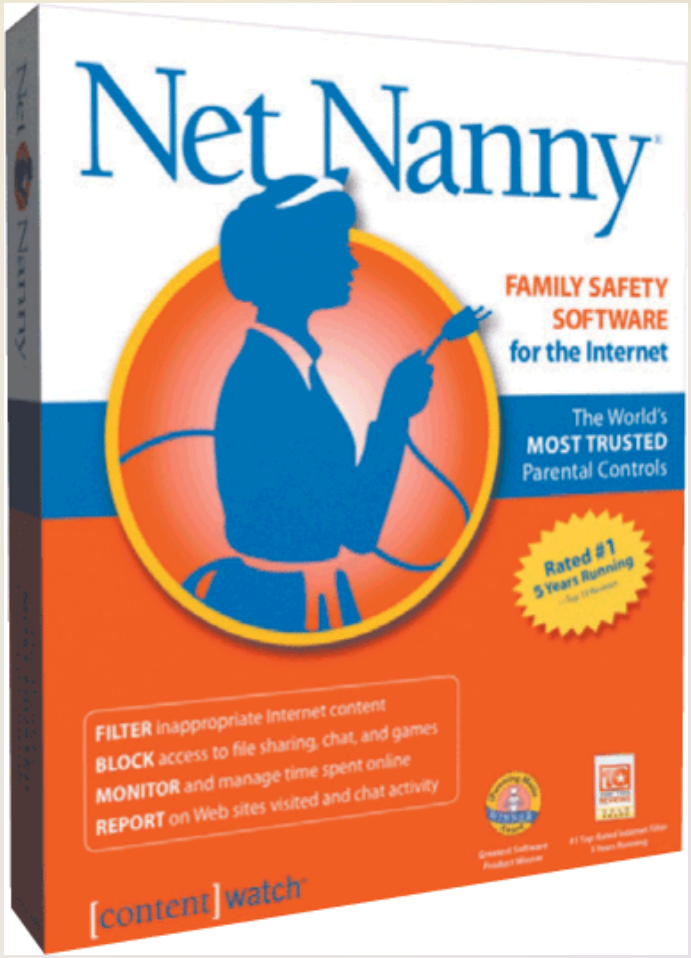
Ethics and Society

Social engineering is defined as gaining unauthorized access or obtaining confidential information by taking advantage of trust and naivety

Employee monitoring involves the use of computers to observe, record, and review an employee's use of a computer

Ethics and Society

- **Content filtering** is the process of restricting access to certain material on the Web
- Many businesses use content filtering
- Internet Content Rating Association (ICRA)
- **Web filtering software** restricts access to specified Web sites



Pages 590 – 591
Figure 11-37

Summary

Potential computer risks and safeguards

Wireless security risks and safeguards

Computer-related health issues and preventions

Ethical issues surrounding information accuracy, intellectual property rights, codes of conduct, green computing, and information privacy

Chapter Eleven

Computer Security and Safety, Ethics, and Privacy

Discovering Computers 2012

Your Interactive Guide to the Digital World

Chapter 11 Complete