Discovering Computers Enhanced Edition ©2017

Tools, Apps, Devices, and the Impact of Technology

Chapter 5

Digital Security, Ethics, and Privacy



Objectives Overview

Define the term, digital security risks, and briefly describe the types of cybercriminals

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

Discuss techniques to prevent unauthorized computer access and use

Explain the ways that software manufacturers protect against software piracy

Discuss how encryption, digital signatures, and digital certificates work

See Page 212
for Detailed Objectives

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Objectives Overview

Identify safeguards against hardware theft, vandalism, and failure

Explain the options available for backing up

Identify risks and safeguards associated with wireless communications

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

Discuss issues surrounding information privacy

See Page 212
for Detailed Objectives

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Digital Security Risks

- A **digital security risk** is any event or action that could cause a loss of or damage to a computer or mobile device hardware, software, data, information, or processing capability
- Any illegal act involving the use of a computer or related devices generally is referred to as a **computer crime**
- A **cybercrime** is an online or Internet-based illegal act

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

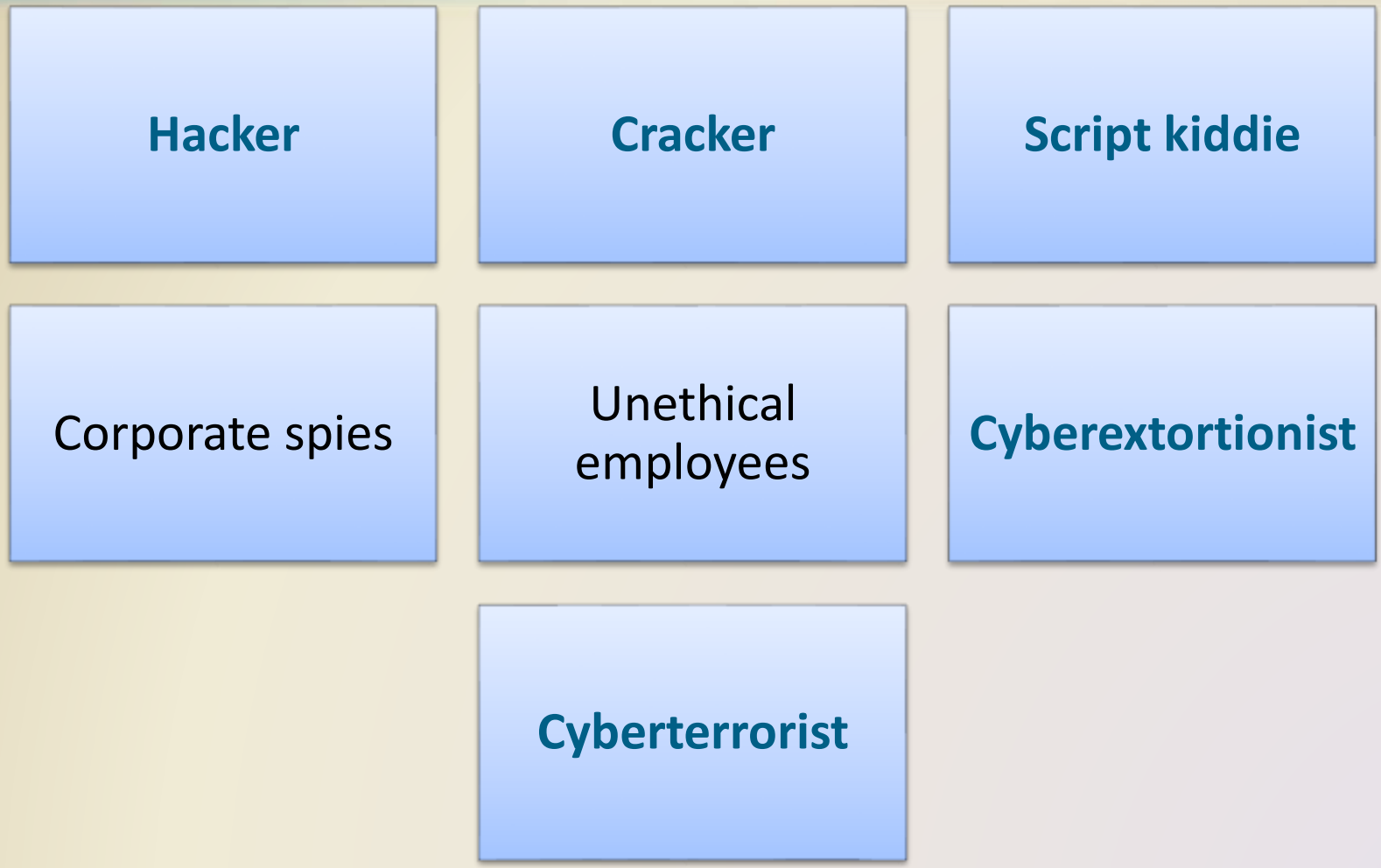
Digital Security Risks



© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Page 213
Figure 5-1

Digital Security Risks



© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Internet and Network Attacks

- Information transmitted over networks has a higher degree of security risk than information kept on an organization's premises
- **Malware**, short for malicious software, consists of programs that act without a user's knowledge and deliberately alter the operations of computers and mobile devices

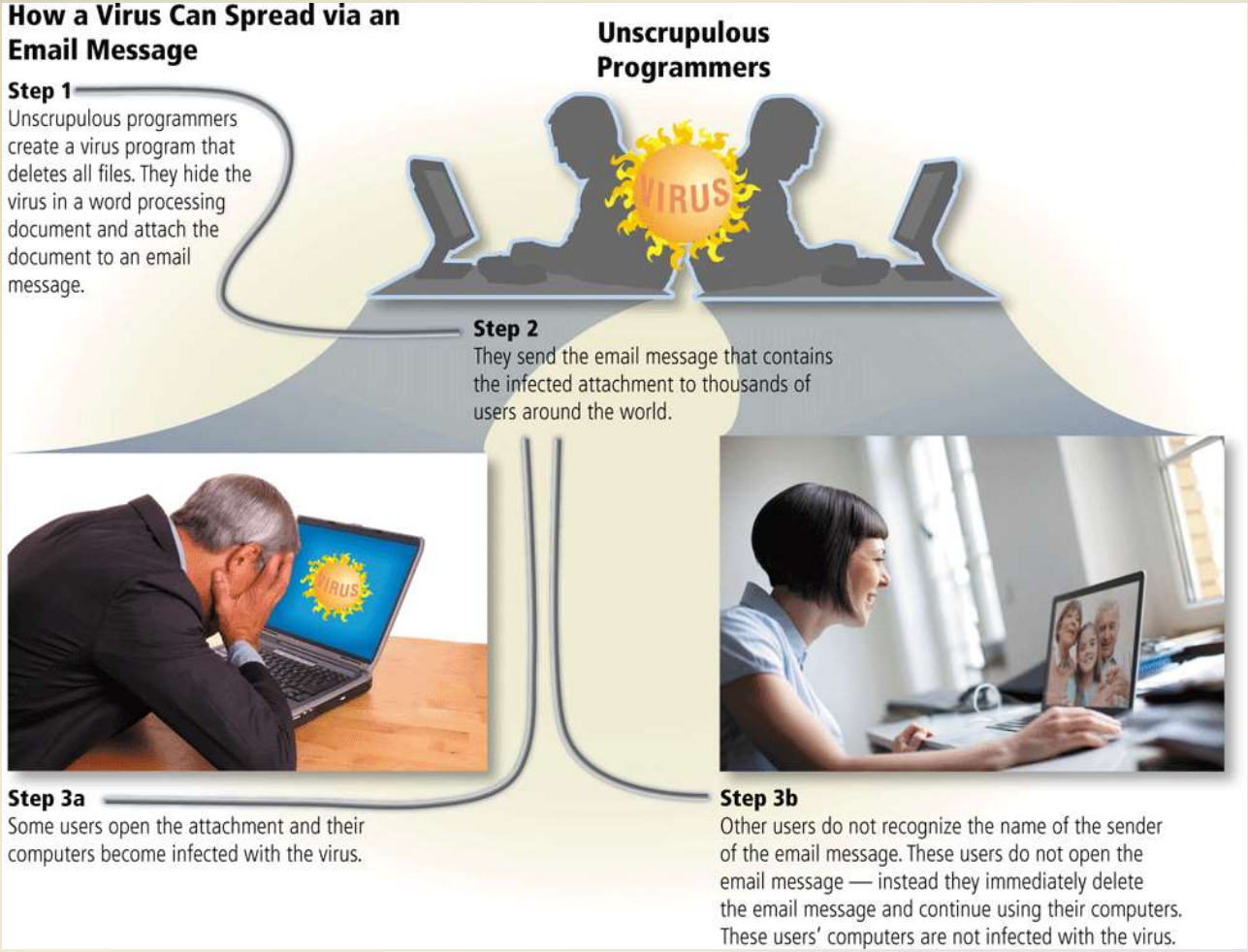
Table 5-1 Common Types of Malware

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

Page 215
Table 5-1

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Internet and Network Attacks



Page 215
Figure 5-2

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Internet and Network Attacks

- A **botnet** is a group of compromised computers or mobile devices connected to a network
  - A compromised computer or device is known as a **zombie**
- A **denial of service attack** (**DoS attack**) disrupts computer access to an Internet service
  - Distributed DoS attack (DDoS attack)
- 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

Pages 216 - 217

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Internet and Network Attacks

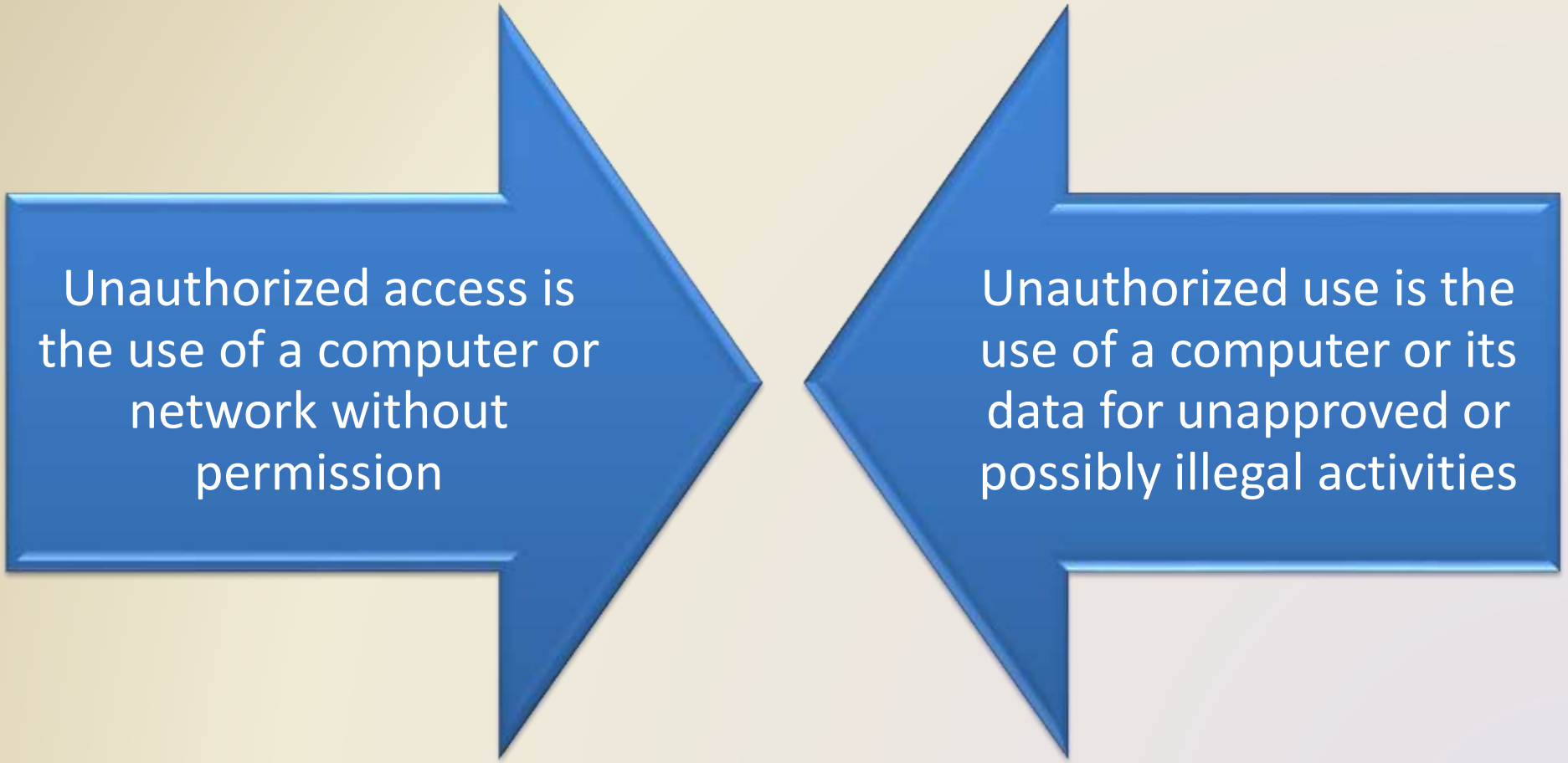
- A **firewall** is hardware and/or software that protects a network's resources from intrusion



Pages 219 - 220
Figure 5-4

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

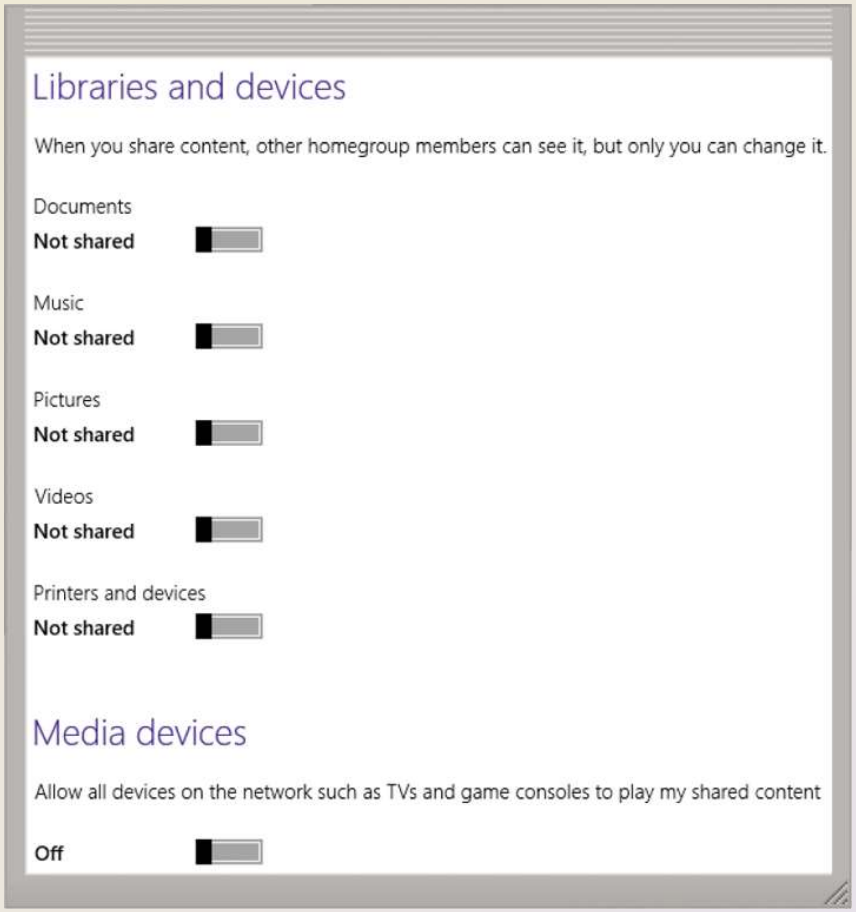
Unauthorized Access and Use



© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Unauthorized Access and Use

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



Page 221
Figure 5-5

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Unauthorized Access and Use

- Access controls define who can access a computer, device, or network; when they can access it; and what actions they can take while accessing it
- The computer, device, or netw ould maintain an audit trail that rec successful and unsuccessful ac
  - **User name**
  - **Password**



Pages 222 - 223
Figure 5-6

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Unauthorized Access and Use

- A passphrase is a private combination of words, often containing mixed capitalization and punctuation, associated with a user name that allows access to certain computer resources
- A **PIN** (personal identification number), sometimes called a passcode, is a numeric password, either assigned by a company or selected by a user
- A possessed object is any item that you must possess, or carry with you, in order to gain access to a computer or computer facility
- 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 or mobile device verifying a physical or behavioral characteristic

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Unauthorized Access and Use

Fingerprint reader

Face recognition system



Hand geometry system

Voice verification system



Signature verification system

Iris recognition system

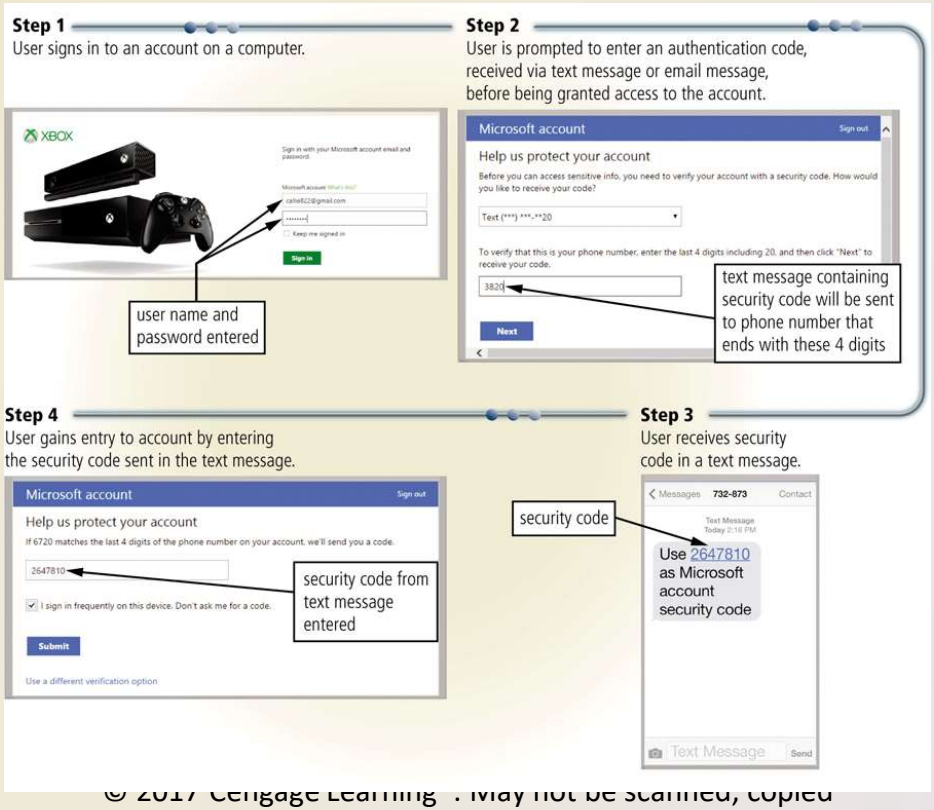


Pages 224 – 226
Figures 5-8 – 5-11

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Unauthorized Access and Use

- **Two-step verification** uses two separate methods, one after the next, to verify the identity of a user

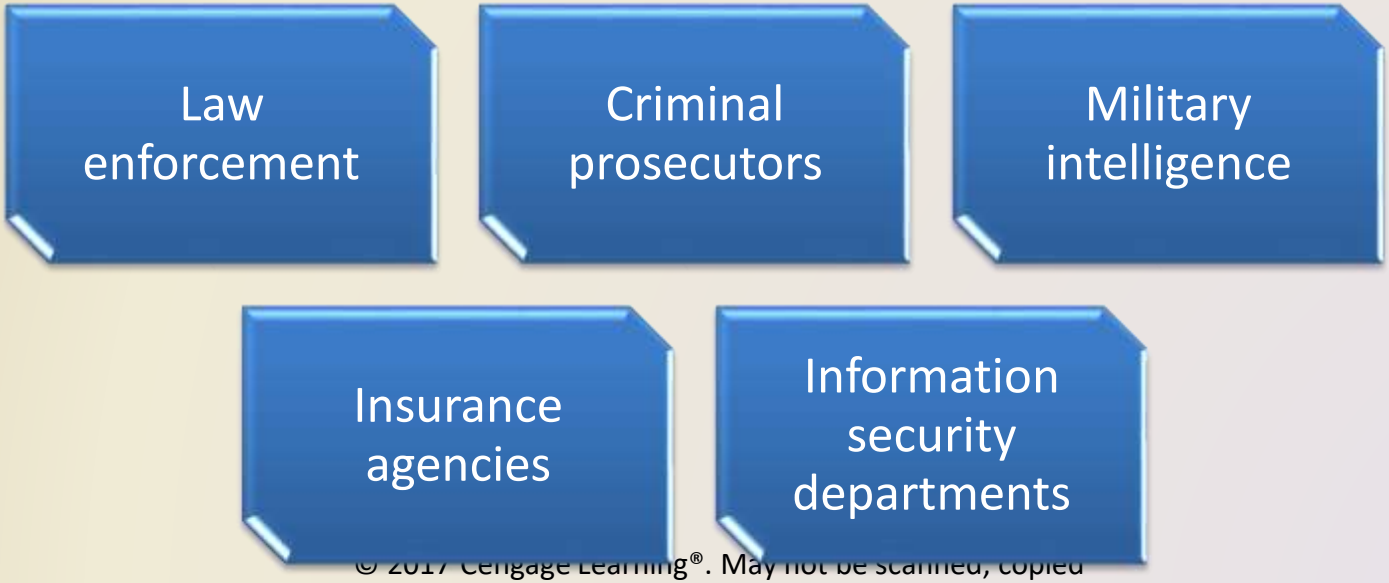


© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Pages 226 – 227
Figure 5-12

Unauthorized Access and Use

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



© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Software Theft

- **Software theft** occurs when someone:

Steals software media

Intentionally erases programs

Illegally registers and/or activates a program

Illegally copies a program

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Software Theft

- Many manufacturers incorporate an activation process into their programs to ensure the software is not installed on more computers than legally licensed
- During the **product activation**, which is conducted either online or by phone, users provide the software product's identification number to associate the software with the computer or mobile device on which the software is installed

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Software Theft

- A **license agreement** is the right to use software

Typical Conditions of a Single-User License Agreement

You can…

- Install the software on only one computer or device. (Some license agreements allow users to install the software on a specified number of computers and/or mobile devices.)
- Make one copy of the software as a backup.
- Give or sell the software to another individual, but only if the software is removed from the user's computer first.

You cannot…

- Install the software on a network, such as a school computer lab.
- Give copies to friends and colleagues, while continuing to use the software.
- Export the software.
- Rent or lease the software.

Pages 228 – 229
Figure 5-13

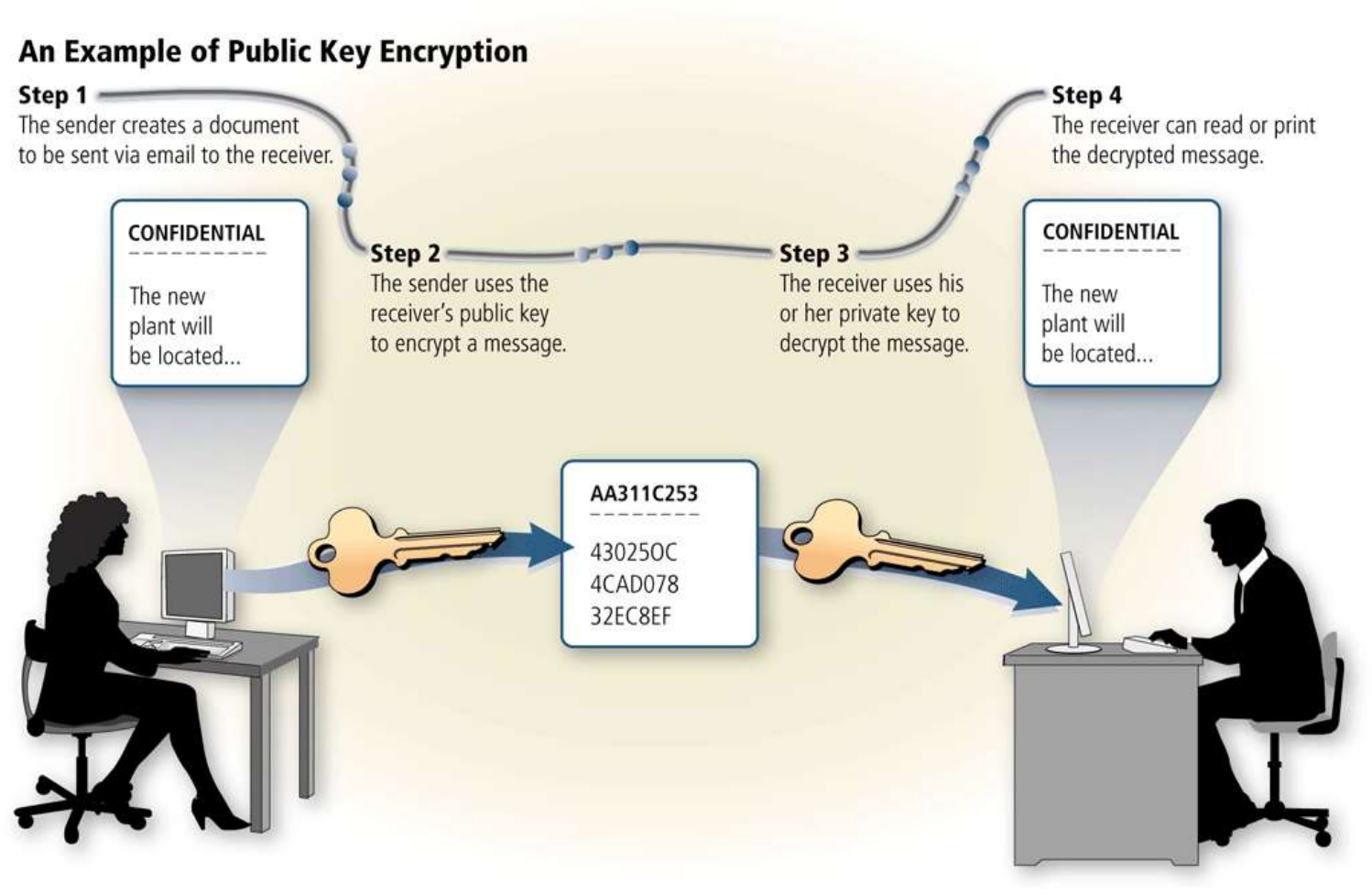
© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Theft

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

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Theft



Page 230
Figure 5-14

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Theft

- A **digital signature** is an encrypted code that a person, website, or organization attaches to an electronic message to verify the identity of the message sender
  - Often used to ensure that an impostor is not participating in an Internet transaction
- A **digital certificate** is a notice that guarantees a user or a website is legitimate
- A website that uses encryption techniques to secure its data is known as a **secure site**

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Theft



© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Page 231
Figure 5-15

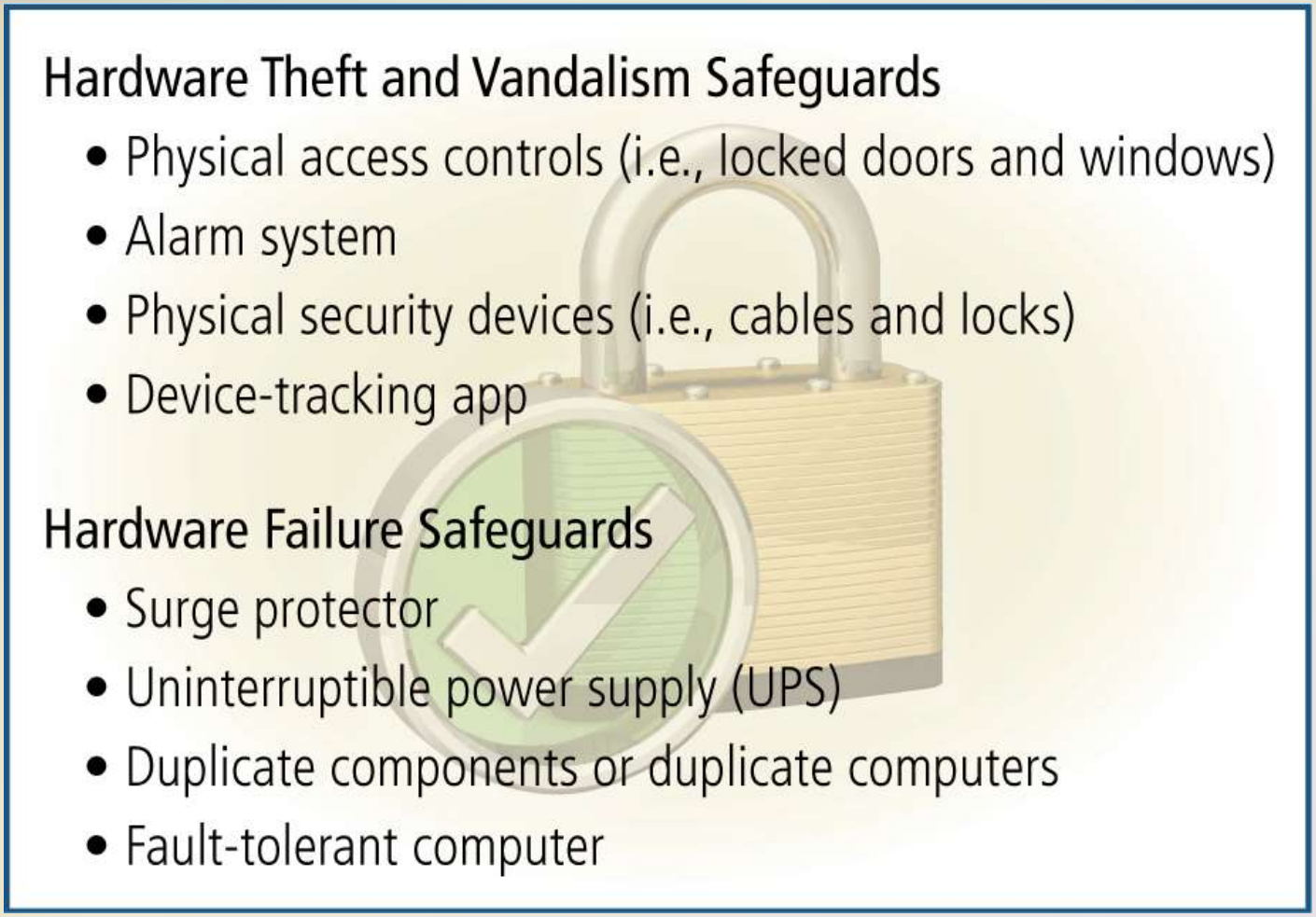
Hardware Theft, Vandalism, and Failure

Hardware theft is the act of stealing digital equipment

Hardware vandalism is the act of defacing or destroying digital equipment

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Hardware Theft, Vandalism, and Failure



Page 233
Figure 5-16

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Backing Up – The Ultimate Safeguard

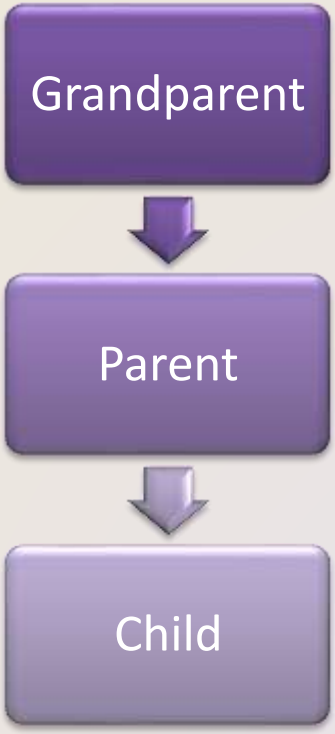
- A **backup** is a duplicate of a file, program, or media that can be used if the original is lost, damaged, or destroyed
  - To **back up** a file means to make a copy of it
- Off-site backups are stored in a location separate from the computer or mobile device site



© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Backing Up – The Ultimate Safeguard

- Categories of backups:
  - Full
  - Differential
  - Incremental
  - Selective
  - Continuous data protection
  - Cloud
- Three-generation backup policy



© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Backing Up – The Ultimate Safeguard

Table 5-2 Various Backup Methods

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

Page 234
Table 5-2

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Wireless Security

- Wireless access poses additional security risks
- Some perpetrators connect to other's wireless networks to gain free Internet access or confidential data
- Others connect to a network through an unsecured wireless access point (WAP) or combination router/WAP



Page 236
Figure 5-18

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Ethics and Society

- **Technology ethics** are the moral guidelines that govern the use of computers, mobile devices, information systems, and related technologies
- Information accuracy is a concern
  - Not all information on the Internet is correct



Pages 238 - 240
Figure 5-20

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Ethics and Society

- Intellectual property refers to unique and original works such as ideas, inventions, art, writings, processes, company and product names, and logos
- Intellectual property rights are the rights to which creators are entitled to their work
- A copyright protects any tangible form of expression
- Digital rights management (DRM) is a strategy designed to prevent illegal distribution of movies, music, and other digital content

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Ethics and Society

- A **code of conduct** is a written guideline that helps determine whether a specification is ethical/unethical or allowed/not allowed

Sample IT Code of Conduct

1. Technology may not be used to harm other people.
2. Employees may not meddle in others' files.
3. Employees may use technology only for purposes in which they have been authorized.
4. Technology may not be used to steal.
5. Technology may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' technology resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use technology in a way that demonstrates consideration and respect for fellow humans.

Page 241
Figure 5-21

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Ethics and Society

- **Green computing** involves reducing the electricity and environmental waste while using computers, mobile devices, and related technologies

Green Computing Tips

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

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Page 241
Figure 5-22

Information Privacy

- **Information privacy** refers to the right of individuals and companies to deny or restrict the collection, use, and dissemination of information about them
- Huge databases store data online
- Websites often collect data about you, so that they can customize advertisements and send you personalized email messages
- Some employers monitor your computer usage and email messages

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

How to Safeguard Personal Information



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

Page 242
Figure 5-23

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

- Information about you can be stored in a database when you:
  - Fill out a printed or online form
  - Create a profile on an online social network
  - Register a product warranty



Pages 242 - 243
Figure 5-24

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

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

Allow for personalization

Store user names and/or passwords

Assist with online shopping

Track how often users visit a site

Target advertisements

Pages 243 - 244

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy



Page 244
Figure 5-25

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

- **Phishing** is a scam in which a perpetrator sends an official looking email message that attempts to obtain your personal and/or financial information
- With clickjacking, an object that can be tapped or clicked on a website contains a malicious program

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

- **Spyware** is a program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online
- **Adware** is a program that displays an online advertisement in a banner or pop-up window on webpages, email messages, or other Internet services

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

- **Social engineering** is defined as gaining unauthorized access to or obtaining confidential information by taking advantage of the trusting human nature of some victims and the naivety of others

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

- The concern about privacy has led to the enactment of federal and state laws regarding the storage and disclosure of personal data
  - See Table 5-3 on page 246 for a listing of major U.S. government laws concerning privacy

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

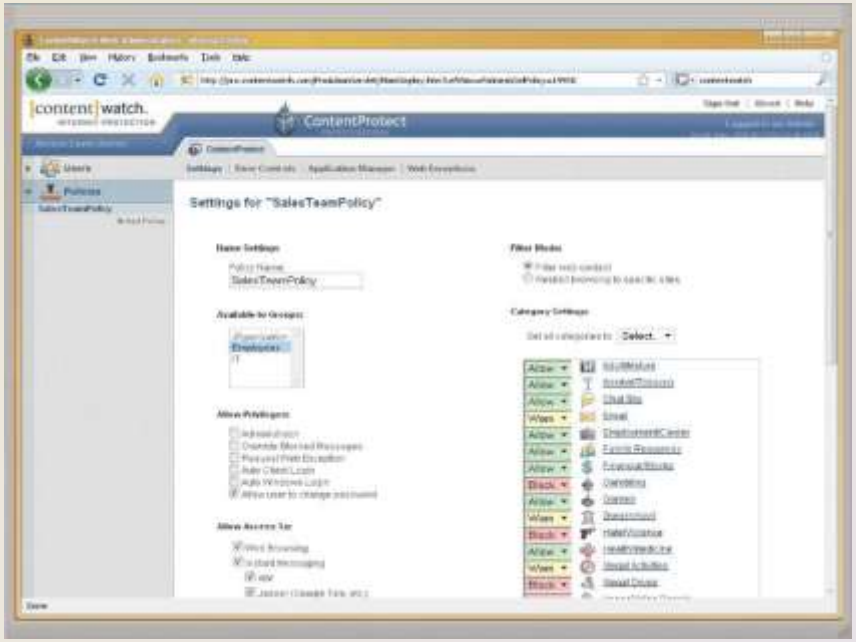
Employee monitoring involves the use of computers, mobile devices, or cameras to observe, record, and review an employee's use of a technology, including communications such as email messages, keyboard activity (used to measure productivity), and websites visited

Many programs exist that easily allow employers to monitor employees. Further, it is legal for employers to use these programs

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Privacy

- **Content filtering** is the process of restricting access to certain material
  - Many businesses use content filtering
- **Web filtering software** restricts access to specified websites



Pages 247 - 248
Figure 5-26

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Summary

- Variety of digital security risks
- Cybercrime and cybercriminals
- Risks and safeguards associated with Internet and network attacks, unauthorized access and use, software theft, information theft, and hardware theft, vandalism, and failure
- Various backup strategies and methods of securing wireless communications
- Ethical issues in society and various ways to protect the privacy of personal information

© 2017 Cengage Learning®. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Discovering Computers Enhanced Edition ©2017

Tools, Apps, Devices, and the Impact of Technology

Chapter 5

Digital Security, Ethics, and Privacy



Chapter 5 Complete