Chapter 9
Security and Privacy

Deborah Morley
Charles S. Parker
Learning Objectives (1)

• Explain why computer users should be concerned about security and privacy as they relate to computing devices, networks, and the Internet.

• Identify some risks associated with hardware loss, hardware damage, and system failure, and understand ways to safeguard a computing device against these risks.

• List several examples of unauthorized access and unauthorized use and explain several ways to protect against them.

• Provide several examples of computer sabotage and explain how individuals and businesses can protect against it.
Learning Objectives (2)

• Discuss online theft, identity theft, spoofing, phishing, and other types of dot cons and detail steps an individual can take to protect against these threats.

• Identify some personal safety risks associated with Internet use and list steps individuals can take to protect themselves.

• Describe some privacy concerns regarding databases, electronic profiling, spam, and telemarketing, and identify ways individuals can protect their privacy.

© 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.
Learning Objectives (3)

• Discuss several types of electronic surveillance and monitoring, and list ways individuals can protect their privacy.

• Discuss the current state of network and Internet security and privacy legislation.
Overview

• This chapter covers:
  – Security concerns stemming from the use of computers, 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
  – Possible risks to personal privacy and precautions that can be taken to safeguard one’s privacy
  – Legislation related to network and Internet security
Why Be Concerned About Computer, Network, And Internet Security And Privacy?

• **Computer crime** (cybercrime) includes any illegal act involving a computer
  – A multibillion-dollar business often performed by criminals

• **Information privacy** refers to the rights of individuals and companies to control how information about them is collected and used
  – The privacy of Web site activities and e-mail messages
  – Security breaches on systems that contain personal information

• All computer users should be aware of security concerns and the precautions that can be taken
Hardware Loss and Damage

• Hardware loss occurs when a personal computer, USB flash drive, smartphone, or other piece of hardware is stolen, damaged, or lost by the owner
  – Both security and privacy concern

• **Hardware theft** refers to hardware stolen from an individual or from a business, school, or other organization
  – Theft for the information contained on computers
    • Risk identity theft and other fraudulent activities
  – Theft for the hardware itself

• Damage can occur from power fluctuations, heat, dust, static electricity, water, and abuse
System Failure and Other Disasters

• **System failure** is the complete malfunction of a computer system
  – Can occur because of a hardware problem, a software problem, or computer sabotage
  – Because of a natural disaster or a terrorist attack
  – Can also lose data due to malfunctioning hardware, accidentally deleting a file, etc.
Protecting Against Hardware Loss, Hardware Damage, and System Failure

• Door and computer equipment locks
  – Locked doors and other access control methods
  – Cable locks permanently secure hardware in schools and businesses
    • Most portable computers come with a security slot
    • Tablets may be used with a security case
  – Laptop alarm software emits a very loud alarm noise
  – Wireless tether systems tie the smartphone to a key fob
  – Important for businesses ensure that employees follow security protocols
Examples of Cable Locks

**FIGURE 9-1**
Cable locks secure computers and other hardware.

**NOTEBOOK LOCKS**
This combination cable lock connects to the security slot built into the notebook computer.

**SECURITY CASES**
This iPad security case/stand encloses the iPad and secures it via a keyed cable lock.
Encryption and Self-Encrypting Hard Drives

- **Encryption** temporarily makes data unreadable to protect that data from unauthorized individuals.
- **Full disk encryption (FDE)** automatically encrypts everything stored on a drive.
  - A hard drive that uses FDE referred to as a **self-encrypting hard drive**
- A password, biometric feature, or PIN number provides access.
Device Tracking Software and Antitheft Tools

- Device tracking software
  - Designed to locate lost or stolen hardware
  - Location typically determined by GPS or Wi-Fi
  - Some display a message on the screen
  - Some remotely lock the device
  - Some have a kill switch that causes the device to self-destruct

![FIGURE 9-3](-source.png)
Proper Hardware Care

• Protective cases protect portable devices from minor abuse
• **Ruggedized devices** withstand much more physical abuse than a conventional computing device
  — Semirugged to ultrarugged
• **Surge suppressors** protect hardware from damage due to electrical fluctuations
• **Uninterruptible power supply (UPS)** contains a built-in battery that provides continuous power to connected components when the electricity goes out
• Unless ruggedized, protect devices against dust, heat, static, moisture, and jostling
Examples of Ruggedized Devices

**FIGURE 9-5**
Ruggedized devices.

**SEMIRUGGED (WATERPROOF)**
SMARTPHONES

**RUGGED TABLETS**
Trend

Kill Switches

- Software that enables owners to render stolen devices inoperable
- The Android Device Manager
  - Displays the current location of a device
  - Can ring the device, lock it, display a message on the lock screen, or erase it
- Some kill switches can actually destroy the device

© 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.
Backups and Disaster Recovery Plans

• Businesses should backup at least per day all new data on a regular basis
• Continuous data protection (CDP) backs up data in real time as it changes
• A disaster recovery plan (business continuity plan) indicates how an organization will recover from a disruptive event
  – Hot sites and cold sites provide alternate location
  – Cloud data recovery services provide copies of data
  – An emergency mail system provider acts as a temporary mail server
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 or acceptable use policies
  – Used to specify rules for behavior, typically by a business or school
Hacking

• **Hacking** involves using a computer to break into another computer system
  – A serious threat for individuals, businesses, and national security, e.g., cyberterrorism
  • Computers controlling power grids, banks, defense systems, and other vital systems
  – Often performed via wireless networks today
    • Wireless networks widely used and easier to hack
    • Many 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

• **Wi-Fi piggybacking**
  – Accessing an unsecured Wi-Fi network from the hacker’s current location without authorization

• Wi-Fi finders can be used to find free and fee-based hotspots
Interception of Communications

• Unsecured messages, files, logon information, etc., can be intercepted as it is being sent over the Internet
  – Unencrypted messages, files, logon information, etc. being sent over a public hotspot or unsecured Wi-Fi network
  – Data located on smartphone being intercepted via Bluetooth
  – Credit and debit card information intercepted during the card verification process
    • Packet-sniffing software at payment terminals
Protecting Against Unauthorized Access and Unauthorized Use

- Access control systems control access to facilities, computer networks, company 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
- In businesses, a comprehensive identity management (IDM) system manages users’ access
Possessed Knowledge Access Systems

- **Possessed knowledge access systems** use information that only the authorized user should know
  - **Passwords** - the most common type of possessed knowledge
    - Secret words or character combinations associated with an individual
    - Typically used in conjunction with a username
  - Passwords should be strong and changed frequently
  - Biggest disadvantage: Any individual possessing the proper password will be granted access
Strategies for Creating Strong Passwords

FIGURE 9-8
Strategies for creating strong passwords.

PASSWORD STRATEGIES

- Make the password at least eight characters and include both uppercase and lowercase letters, as well as numbers and special symbols.

- 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@”.

- Develop a system using a basic password for all Web sites plus site-specific information (such as the first two letters of the site and a number you will remember) to create a different password for each site, but still ones you can easily remember. For instance, you can combine your dog’s name with the site initials followed by a number that is significant to you to form a password such as “RoverAM27” for Amazon.com.

- 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 or use a password manager program.

- Use a different password for your highly sensitive activities (such as online banking or stock trading) than for other Web sites. If a hacker determines your password on a low-security site (which is easier to break into), 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—at least every 6 months.
Possessed Object Access Systems

- **Possessed object access systems** use a physical object an individual has in his/her possession to identify that individual
  - Objects are swiped through or placed close to a reader
    - Smart cards, RFID-encoded badges, USB security keys, smartphones
  - Disadvantage: Anyone using object is granted access
Biometric Access Systems

• **Biometric access systems** identifies users by a particular unique biological characteristic
  – Fingerprint, hand, face, iris, voice, etc.
  – Performs both identification and authentication
  – Data read by biometric reader must match what is stored in a database
  – Very high accuracy and biometric characteristic cannot be lost
  – Disadvantages: More expensive and the data cannot be reset if compromised
Examples of Biometric Access Systems

**FIGURE 9-10**

Biometric access and identification systems.

**FINGERPRINT READERS**
Typically used to protect access to work facilities or computers, to log on to secure Web sites, for law enforcement identification, and to pay for products or services.

**FACE RECOGNITION SYSTEMS**
Typically used to control access to highly secure areas, to identify individuals for law enforcement purposes, and to log on to devices or apps, as shown here.
Two-Factor Authentication

- **Two-factor authentication** uses two different methods to authenticate users
  - More secure because hackers are less likely to have both factors
  - Often a username and password in conjunction with a possessed object or biometric characteristic
    - Sometimes the possessed object generates a one-time password (OTP) that must be used to log on
  - Use is growing
  - An option for some Web sites (banking, social media, etc.)
Example of Facebook Two-Factor Authentication

**FIGURE 9-11**
Facebook two-factor authentication.
Controlling Access to Wireless Networks

• Important to secure wireless networks to protect against unauthorized access
  – Implement WPA or WPA2 security
    • Network key is then required for access
  – Can hide network name (SSID) to prevent war driving or Wi-Fi piggybacking
    • Authorized users will need to supply the SSID to access the network
Example of Accessing a Wi-Fi Network

**FIGURE 9-12**
Accessing a Wi-Fi network.
How It Works

Securing a Wireless Home Router

• Use router’s configuration screen
• Be sure to change the password
• Enter the desired SSID name, select the security mode, and type a secure passphrase
• Can use MAC (Media Access Control) address filtering

Configuring a home router.
Firewalls

- **Firewalls** are a collection of hardware and/or software intended to protect a computer or computer network from unauthorized access
  - Typically two-way: Check all incoming (from the Internet) and outgoing (to the Internet) traffic
  - Important for home computers that have a direct Internet connection, as well as for businesses
  - Work by closing down external communications ports
- Intrusion prevention system (IPS) software monitors traffic to detect and block possible attacks
Example of a Personal Firewall

**FIGURE 9-13**
A personal firewall.

**FIREWALL ALERTS**
You are notified when a new program requests access.

**FIREWALL SETTINGS**
You can specify settings for individual programs if desired.
Encryption

• Encryption makes data unreadable to unauthorized individuals
  – Used with secure Wi-Fi networks and VPNs to secure data that is transferred over those networks
  – **Secure Web pages** use encryption in order to protect information transmitted via that Web page
    • Transport Layer Security (TLS) (Secure Sockets Layer (SSL))
  – Self-encrypting hard drives automatically encrypt all content stored on those drives
  – Can be used with stored files as well as files sent over the Internet
Types of Encryption

• **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

• **Public key encryption** (asymmetric key encryption)
  – Uses two keys (a private key and a public key) to encrypt and decrypt documents
    • Public key encrypts file
    • Private key decrypts file
  – Key pairs are obtained through a Certificate Authority

• There are various strengths of encryption available
Example of Public Key Encryption

FIGURE 9-14
Using public key encryption to secure an e-mail message in Microsoft Outlook.
Additional Precautions

• Individuals using public hotspots should use a firewall, VPN, and encryption
  – Turn off automatic Wi-Fi connections, disable ad hoc connections, and turn off file sharing and Bluetooth

• Employers should:
  – Screen potential new hires carefully
  – Limit employee access to only the resources needed
  – Use software to manage devices and prevent data leaks
    • Mobile device management (MDM) – BYOD
    • Data leakage prevention systems
    • Enterprise rights management software
Example of Mobile Device Management (MDM) Software

**FIGURE 9-15**
Mobile device management (MDM) software. Secures and manages the mobile devices used in an organization.
Quick Quiz (1)

1. Many businesses today are requiring that all portable computers and mobile devices issued to employees be ____ in order to protect against a data breach if the device is lost or stolen.
   a. ruggedized
   b. encrypted
   c. formatted

2. True or False: The act of breaking into another computer system is called two-factor authentication.

3. A(n) __________ creates a barrier between a computer and the Internet to protect against unauthorized access.

Answers:
1) b; 2) False; 3) firewall
Computer Sabotage

- **Computer sabotage** refers to acts of malicious destruction to a computer or computer resource
  - Launching a malicious program
  - Altering the content of a Web site
  - Changing data or programs located on a computer

- **A botnet** is 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 spread malware
Malware

• **Malware** is any type of malicious software
  – Written to perform destructive acts (damaging programs, deleting files, erasing drives, etc.)
  • Can take place immediately after infection or at a later time
    – Logic bomb: Triggered when a certain condition is met
    – Time bomb: Triggered by a particular date or time
  – Writing malware is considered unethical; distributing is illegal
  – Is very costly to businesses
Computer Viruses and Computer Worms

• A **computer virus** is 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)
  – Spread when the infected file reaches a new device

• A **computer worm** is a malicious program designed to spread rapidly by sending copies of itself to other computers via a network
  – Typically sent as an e-mail attachment
How a Computer Virus Might Spread

**FIGURE 9-16**
How a computer virus or other type of malicious software might spread.

1. A computer virus originates when an unscrupulous programmer intentionally creates it and embeds it in a file. The infected file is then posted to a Web page where it will be downloaded via the Internet or is sent as an e-mail attachment to a large group of people.

2. When the infected file is opened, the virus copies itself to that device’s hard drive and the device is infected. The virus may then e-mail itself to people in the newly infected device’s e-mail address book or copy itself to any removable storage medium inserted into that device.

3. A virus can spread very quickly because every device that comes in contact with the virus—whether through an infected removable storage medium, infected downloaded file, or infected e-mail attachment—becomes infected, unless antivirus software is used to prevent it.

© 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.
Trojan Horses and Mobile Malware

- A **Trojan horse** is a malicious program that masquerades as something else, usually an application program
  - Rogue anti-malware apps (scareware)
  - Ransomware
  - Spread via downloaded files, e-mail attachments, etc.
- Mobile malware infects smartphones, tablets, etc.
  - Primary goal is to obtain mobile banking credentials
Denial of Service (DoS) Attacks

- **Denial of service (DoS) attacks** are acts of sabotage that attempt to flood a network server or Web server with so much activity that it cannot function
  - Server either shuts down or can no longer handle requests
  - Legitimate users are denied service
  - Distributed DoS (DDoS) attacks are carried out via multiple computers
    - Often botnets
  - Costly in terms of lost business and the time and expense to bring the server back online
Example of a Denial of Service (DoS) Attack

1. Hacker’s computer sends several simultaneous requests; each request asks to establish a connection to the server but supplies false return information. In a distributed DoS attack, multiple computers send multiple requests at one time.

   Hello? I’d like some info...

2. The server tries to respond to each request but can’t locate the computer because false return information was provided. The server waits for a short period of time before closing the connection, which ties up the server and keeps others from connecting.

   I can’t find you, I’ll wait and try again...

3. The hacker’s computer continues to send new requests so, as a connection is closed by the server, a new request is waiting. This cycle continues, which ties up the server indefinitely.

   Hello? I’d like some info...

4. The server becomes so overwhelmed that legitimate requests cannot get through and, eventually, the server usually crashes.

**FIGURE 9-18**

How a denial of service (DoS) attack might work.
Data, Program, or Web Site Alteration

- Hacker can 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
  - Hacking into and changing social networking account contents (Facebook pages, Twitter tweets, etc.)
  - Altering legitimate site to perform malware attacks
    - Estimated that more than half of malicious sites are actually legitimate sites that were compromised
Protecting Against Computer Sabotage: Security Software

• **Security software** is typically a suite of programs used to protect your computer against a variety of threats
  – **Antivirus software** is 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
  – Antispyware software detects and removes spyware
  – Mobile security software protects mobile devices
Other Precautions Against Computer Sabotage

• Control access to computers and networks
• Intrusion protection systems can help businesses detect and protect against denial of service (DoS) attacks
  – Sometimes included in personal security software
• Most Web browsers have security settings
  – To prevent programs from being installed without permission, etc.
Examples of Security Software

FIGURE 9-19
Security software.
Quick Quiz (2)

1. Which product is *not* an example of security software?
   a. antivirus software
   b. ransomware
   c. antispyware software

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** is a fraud or scam carried out through the Internet
- Data theft or information theft
  - Stealing an actual computer or mobile device and then accessing the data on that device
  - Hacking into a device and stealing data or intercepting data as it is being transmitted
  - Common types include customer data (Web site passwords, credit card information, etc.) and proprietary corporate information
Identity Theft

- **Identity theft** involves using someone else’s identity to purchase goods or services, obtain new credit cards or bank loans, or illegally masquerade as that individual.
  - Information can be obtained:
    - Online via hacking, spyware, etc.
    - Via offline documents gathered via trash dumpsters, mailboxes, etc.
    - Via skimming devices
    - Via social engineering and social media
  - Expensive and time consuming to recover from
Example of 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 makes purchases, opens new credit card accounts, and more in the victim’s name. Often, the thief changes the address on the account to delay discovery.

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.

**FIGURE 9-21**

How identity theft works.
Inside the Industry

Skimming and EMV

- Skimming is stealing identifying information from a credit or debit card
- Often occurs at ATM machines that have been compromised
- EMV cards are embedded with a chip that encrypts personal data so that it cannot be easily stolen
  - Card is inserted into payment terminal
  - Generates a unique transaction code every time the card is used

EMV cards protect against skimming and fraudulent transactions.
Phishing and Spear Phishing

- **Phishing** is the use of spoofed communications to gain credit card numbers and other personal data
  - Often via e-mail; typically looks legitimate but links go to a spoofed Web site
  - Information obtained is used in identity theft or fraud
  - Can occur via spyware, text messages, social media messages, etc.
  - Typosquatting: Setting up spoofed Web sites with URLs slightly different from legitimate sites

- **Spear phishing**
  - A personalized phishing scheme targeted to specific individuals
Example of a Phishing E-Mail

**FIGURE 9-22**
Phishing. Phishing schemes typically use legitimate-looking e-mails to trick users into providing private information.

The link is for a non-secure Web page and does not use the bank’s domain.

This e-mail looks legitimate, but the link goes to a spoofed Web page.
Social Media Hacking and Pharming

- **Social media hacking** is the act of accessing someone else’s social media account to post comments or send messages as that individual
  - Often used with phishing

- **Pharming** is 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)
    - Can be root DNS servers or a company DNS server
  - Pharmers can capture logon information, etc.
Online auction fraud occurs when an item purchased through an online auction is never delivered or the item is not as specified
  – Illegal, but as with other types of online fraud, prosecution is difficult

Other Internet scams:
  – Loan and pyramid scams
  – Work-at-home cons
  – Nigerian letter fraud schemes
  – Online romance scams
  – Fake job site postings
Protecting Against Online Theft, Online Fraud, and Other Dot Cons

• General precautions
  – Do not disclose personal information unless it is absolutely necessary and you know how the information will be used
  – Shred documents containing personal information
  – Watch bills and credit report to detect identity theft early
  – Order a full credit history on yourself a few times a year to check for accounts listed in your name
  – Never click a link in an e-mail message to go to a secure Web site—always type the URL in the browser instead
  – Act quickly if you think you have been a victim
**Tips for Avoiding Identity Theft**

<table>
<thead>
<tr>
<th>TIPS FOR AVOIDING IDENTITY THEFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect your Social Security number—give it out only when necessary.</td>
</tr>
<tr>
<td>Be careful with your physical mail and trash—shred all documents containing sensitive data.</td>
</tr>
<tr>
<td>Secure your computer—update your operating system and use up-to-date security (antivirus, antispyware, firewall, etc.) software.</td>
</tr>
<tr>
<td>Be cautious—never click on a link in an e-mail message or respond to a too-good-to-be-true offer.</td>
</tr>
<tr>
<td>Use strong passwords for your computer and online accounts.</td>
</tr>
<tr>
<td>Verify sources before sharing sensitive information—never respond to e-mail or phone requests for sensitive information.</td>
</tr>
<tr>
<td>Be vigilant while on the go—safeguard your wallet, smartphone, and portable computer.</td>
</tr>
<tr>
<td>Watch your bills and monitor your credit reports—react immediately if you suspect fraudulent activity.</td>
</tr>
</tbody>
</table>
Tips for Identifying a Phishing E-Mail

A PHISHING E-MAIL OFTEN . . .

Tries to scare you by stating that your account will be closed or that you are a victim of fraud.

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

Contains a bogus link (point to a hyperlink in the message to view the URL for that link—a phisher would have to use a URL like microsoft.phisher.com, not microsoft.com).

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

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

Contains spelling or grammatical errors.
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:
  - Analyze user’s habits to look for suspect activity.
  - Add additional steps in their logon process to prove it’s not a phishing site.
  - Authenticate new devices with cognitive authentication questions.
Digital IDs

• A **digital ID (digital certificate)** is a group of electronic data that can be used to verify the identity of a person or organization
  – 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/TLS or EV SSL
  – Includes public/private key pair
    • Can be used to encrypt files
    • Can be used to add a **digital signature** to an e-mail message or other document
      – Private key signs; public key verifies the signature
      – Guarantees the document was not altered after it was signed
Example of an EV SSL Certificate

FIGURE 9-27
EV SSL certificates. The browser’s Address bar reflects information about the digital certificate being used.
Personal Safety Issues: Cyberbullying

- **Cyberbullying** involves the use of online communications to bully another person
  - E-mail, social media, etc.
  - Often anonymous
  - Prevalent among teens; estimated to affect more than one-third of all U.S. teenagers
Cyberstalking

- **Cyberstalking** involves repeated threats or other malicious behavior that poses a credible threat of harm carried out online
  - Cyberstalking typically begins with online harassment and can lead to offline stalking and possibly physical harm
  - Victims can be personal or found online
  - Although there are no specific federal laws against cyberstalking, all states have made it illegal
  - Federal laws apply if online actions include a computer crime, suggest a threat of personal injury, or involve sending obscene e-mail messages
Sexting, Sextortion, and Online Pornography

• Sexting is the act of sending sexually explicit photos or messages (sexts) to others
  – The sender of a compromising photo or message loses control of it and it can live on the Internet forever

• Sextortion occurs when someone who sees a sext threatens to expose it unless the individual sends more explicit photos

• Online pornography
  – Attempts to ban this type of material from the Internet have not been successful
  – Online pornography involving minors is illegal
Protecting Against Cyberbullying, Cyberstalking, and Other Personal Safety Concerns

- Many social networking sites have privacy features
- Numerous states have implemented cyberbullying and cyberstalking laws
- Common-sense precautions should be taken

**ONLINE SAFETY TIPS**

- Be cautious and discreet online; use gender-neutral, nonprovocative identifying names, such as jsmith, instead of janessmith 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.
- Do not respond to any insults or other harassing comments you may receive online.
- Do not include personal information on social media that could be used by an online stalker.
- Do not send sexts to others.
- Be sure to monitor childrens’ computer and smartphone activities.
- Be sure to give children and teens computer use guidelines, including which types of online activities are allowed and which ones are not allowed, to never reveal personal information about themselves online, and to always tell an adult if an online individual requests personal information, a meeting, or issues a threat.

**FIGURE 9-29**
Some tips to keep you safe online.
Quick Quiz (3)

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. spamming
   c. phishing

2. True or False: Cyberstalking can lead to offline stalking and sometimes even the death of the victim.

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
Databases and Electronic Profiling

- **Marketing databases** contain marketing and demographic data; where people live and what products they buy
- **Government databases**: A collection of data about people that is collected and maintained by the government
  - Some information available to the public, including marketing companies and database search services
- **Electronic profiling**: Collecting in-depth information about an individual; name, address, income, and buying habits
  - Information is sold to companies upon request to be used for marketing purposes
- Most business Web sites have a **privacy policy** that explains how personal information is used and share
Examples of Databases Available via the Internet

FIGURE 9-30
A variety of searchable databases are available via the Internet.
Spam and Other Marketing Activities

- **Spam** refers to unsolicited e-mail sent to a large group of individuals at one time
  - The electronic equivalent of junk mail
  - At best, an annoyance to recipients
  - At worst, can disable a mail network completely

- One of the most common ways of getting on a spam mailing list is by having your e-mail address entered into a marketing database

- While most spam is legal, the CAN-SPAM Act of 2003 established requirements for commercial e-mailers
Examples of Spam

**FIGURE 9-31**
Examples of spam.
Protecting the Privacy of Personal Information

• Use private browsing mode offered by some browsers
• Safeguard your e-mail address
  – Use one e-mail address for trusted sources
  – Use a throw-away e-mail address for activities that lead to junk e-mail
  – Never reply to or try to unsubscribe from any spam
• Be cautious about revealing personal information
• Use an e-mail filter and/or spam filter to sort e-mail
• Opt out to remove yourself from marketing lists

© 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.
Tips for Safeguarding Personal Information

TIPS FOR PROTECTING PERSONAL INFORMATION

Read a Web site’s privacy policy before providing any personal information to see if the Web site reserves the right to share your information with others—if so, do not use the site if that is unacceptable to you.

Avoid putting too many personal details on your Web site or a social media site.

Avoid using location-based services that share your location information with strangers, and check the privacy options for the sites you use to limit who can see the content that you post.

Use your throw-away e-mail address when you sign up for free trials or other services that may result in spam.

Consider using privacy software, such as Privacy Guardian, to hide your personal information as you browse the Web so it is not revealed and your activities cannot be tracked by marketers.

Supply only the required information when you are completing an online form; if you are asked for more personal information than you are comfortable providing, don’t use the site.

Unless you are using private browsing, use browser options to delete any personal information and settings stored on a public computer at the end of your session, and be sure to log out of any Web sites you were using before leaving the computer.
Protecting the Privacy of Personal Information (cont’d)

• Business must use adequate security measures
  – Secure servers and encryption can protect the data stored on a server
  – Firewalls and access systems can protect against unauthorized access

• Properly dispose of hardware containing data
  – Papers, CDs, DVDs, and other media should be shredded
  – Hard drives should be wiped—overwritten several times using special disk-wiping or disk-erasing software
  – A data destruction service can be used to shred hard drives
Example of a Shredded Hard Drive

**FIGURE 9-34**
Shredded hard drives.

BEFORE SHREDDING

AFTER SHREDDING

© 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.
Electronic Surveillance and Monitoring

• Electronic tools can be used to watch individuals, listen to their conversations, monitor their activities, etc.

• **Computer monitoring software** is used for monitoring someone’s computer activity
  – Some can block specific Web sites
  – Some notify a designated party of the use of specified keywords or inappropriate Web sites
  – Keystroke logging software can be used to record e-mail messages and documents before they are encrypted
  – Used by parents, spouses, law enforcement agencies, and employers
Example of Computer Monitoring Software

**FIGURE 9-35**

Computer monitoring software. Can be used to monitor employee computer activity, as shown here.

The current tab shows the top Web sites visited by employees.

Click to view screenshots of employee activities.

[Image of computer monitoring software interface]

Source: ActivTrak.com
Video Surveillance

• **Video surveillance** is the use of video cameras to monitor activities
  – For security and law enforcement purposes
  – Used in businesses, schools, outdoors, etc.
  – With face recognition technology, it can help detect suspicious behavior

• Privacy concerns
  – How captured video is used
  – How mobile device cameras are used
Public Video Surveillance

![Public Video Surveillance Sign](image)

**FIGURE 9-36**
Public video surveillance is common in metropolitan areas.
Technology and You

Wearables and Privacy

• Some wearable devices discreetly gather data about individuals
  – Google Glass
  – Audio recording devices like Kapture

• Another privacy concern is what is being done with the vast amount of data your wearables gather about you

Audio recording devices like Kapture can record the conversations of others.
Employee Monitoring

• **Employee monitoring** involves recording or observing the actions of employees while on the job
  – Screening telephone calls, reviewing e-mail, tracking computer and Internet usage

• Tools that can monitor the physical locations of employees
  – Video cameras
  – Smart or RFID-enabled ID cards (sometimes called proximity cards)
  – GPS systems that track an employee via his or her smartphone
Presence Technology

- **Presence technology** is the ability of one computing device to identify another device on the same network and determine its status
  - Integrated into many messaging programs, like Facebook
  - Used in some business communications programs
- Privacy advocates are concerned about the use of this technology
Protecting Personal and Workplace Privacy

• The employer’s responsibilities
  – Keep private information about their employees, the company, and their customers safe
  – Take precautions against both intentional and accidental breaches of privacy by employees
  – Maintain a safe and productive workplace environment

• The employees’ responsibilities
  – Read the company’s employee policy
  – Not violate any company rules while working for that organization
  – Avoid personal activities at work
Network and Internet Security and Privacy Legislation

• Computer security, Internet security, and personal privacy has led state and federal legislators to pass a variety of laws since the 1970s
• Congress has had difficulty passing new legislation related to network and Internet security and privacy
• Privacy is difficult to define and there is a struggle to balance protection with freedom of speech and other civil liberties
  – Involves weighing the need to implement legislation versus the use of voluntary methods to protect computer security and personal privacy
Examples of Computer and Internet Security and Privacy Legislation

<table>
<thead>
<tr>
<th>DATE</th>
<th>LAW AND DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>American Recovery and Reinvestment Act</td>
</tr>
<tr>
<td></td>
<td>Requires HIPAA covered entities to notify patients when protected health information has been compromised.</td>
</tr>
<tr>
<td>2006</td>
<td>U.S. SAFE WEB Act of 2006</td>
</tr>
<tr>
<td></td>
<td>Grants additional authority to the FTC to help protect consumers from spam, spyware, and Internet fraud and deception.</td>
</tr>
<tr>
<td>2005</td>
<td>Real ID Act</td>
</tr>
<tr>
<td></td>
<td>Establishes national standards for state-issued driver's licenses and identification cards.</td>
</tr>
<tr>
<td>2004</td>
<td>Identity Theft Penalty Enhancement Act</td>
</tr>
<tr>
<td></td>
<td>Adds extra years to prison sentences for criminals who use identity theft (including the use of stolen credit card numbers) to commit other crimes.</td>
</tr>
<tr>
<td>2003</td>
<td>CAN-SPAM Act</td>
</tr>
<tr>
<td></td>
<td>Implements regulations for unsolicited e-mail messages and lays the groundwork for law enforcement.</td>
</tr>
<tr>
<td>2003</td>
<td>Do Not Call Implementation Act</td>
</tr>
<tr>
<td></td>
<td>Amends the Telephone Consumer Protection Act to implement the National Do Not Call Register.</td>
</tr>
<tr>
<td>2003</td>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
</tr>
<tr>
<td></td>
<td>Includes a Security Rule that sets minimum security standards to protect health information.</td>
</tr>
<tr>
<td>2003</td>
<td>PROTECT Act</td>
</tr>
<tr>
<td></td>
<td>Amends provisions to prohibit virtual child pornography.</td>
</tr>
<tr>
<td>2002</td>
<td>Sarbanes-Oxley Act</td>
</tr>
<tr>
<td></td>
<td>Requires schools and libraries that receive discounts through the E-rate program to filter obscene content.</td>
</tr>
<tr>
<td>2001</td>
<td>USA PATRIOT Act</td>
</tr>
<tr>
<td></td>
<td>Requires schools and libraries that receive discounts through the E-rate program to filter obscene content.</td>
</tr>
<tr>
<td>2000</td>
<td>Children's Internet Protection Act (CIPA)</td>
</tr>
<tr>
<td></td>
<td>Requires schools and libraries that receive discounts through the E-rate program to filter obscene content.</td>
</tr>
</tbody>
</table>

**FIGURE 9-38**
Computer and Internet security and privacy legislation.
1. The ability of a computing device to identify another device on the same network and determine its status is called __________.
   a. computer monitoring  
   b. video surveillance  
   c. presence technology

2. True or False: A throw-away email can help to reduce spam.

3. A tool that automatically sorts incoming email messages based on specified criteria is a(n) __________.

Answers:
1) c; 2) True; 3) e-mail filter
Summary (1)

• Why Be Concerned About Network and Internet Security?
• Hardware Loss, Hardware Damage, and System Failure
• Unauthorized Access and Unauthorized Use
• Computer Sabotage
• Online Theft, Online Fraud, and Other Dot Cons
• Personal Safety Issues
• Databases, Electronic Profiling, Spam, and Other Marketing Activities
Summary (2)

- Electronic Surveillance and Monitoring
- Network and Internet Security Legislation