

16<sup>th</sup> Edition

# Understanding Computers

Today and Tomorrow

Comprehensive

## Chapter 9

# Security and Privacy

Deborah Morley  
Charles S. Parker

© 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.



# Computer Crime & 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 activities and e-mail messages
  - Security breaches on systems that contain personal information
  - **ACM Code of Ethics 1.1:** *“An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy.”*
- 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 => Disasters & Attacks

- **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.

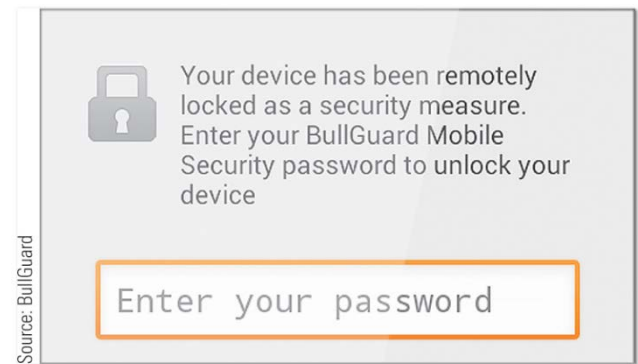


# Physical Security First

- 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

# 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

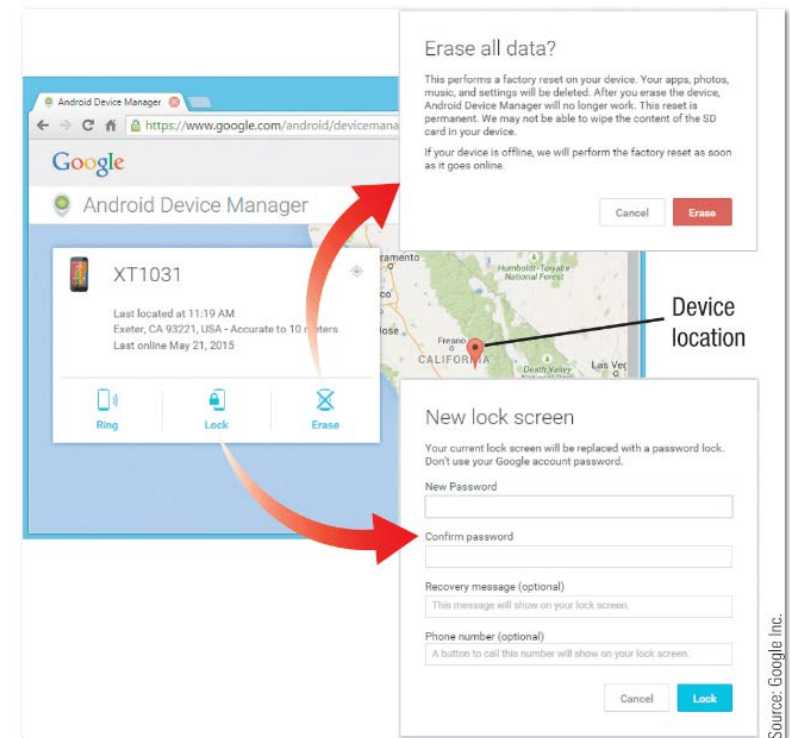


**FIGURE 9-3**  
Remote locking.

# Kill Switches

## 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



The Android Device Manager.



# 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





# Backups and Disaster Recovery Plans

- **Backups**
  - Businesses should backup at least per day all new data on a regular basis
  - Review 3 different backups presented in Storage & OS
- **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

**FIGURE 9-7**

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



Source: JtWire: Chardchanin/Shutterstock.com



# Interception of Communications (Integrity)

- Unencrypted, unsecured 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



# 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

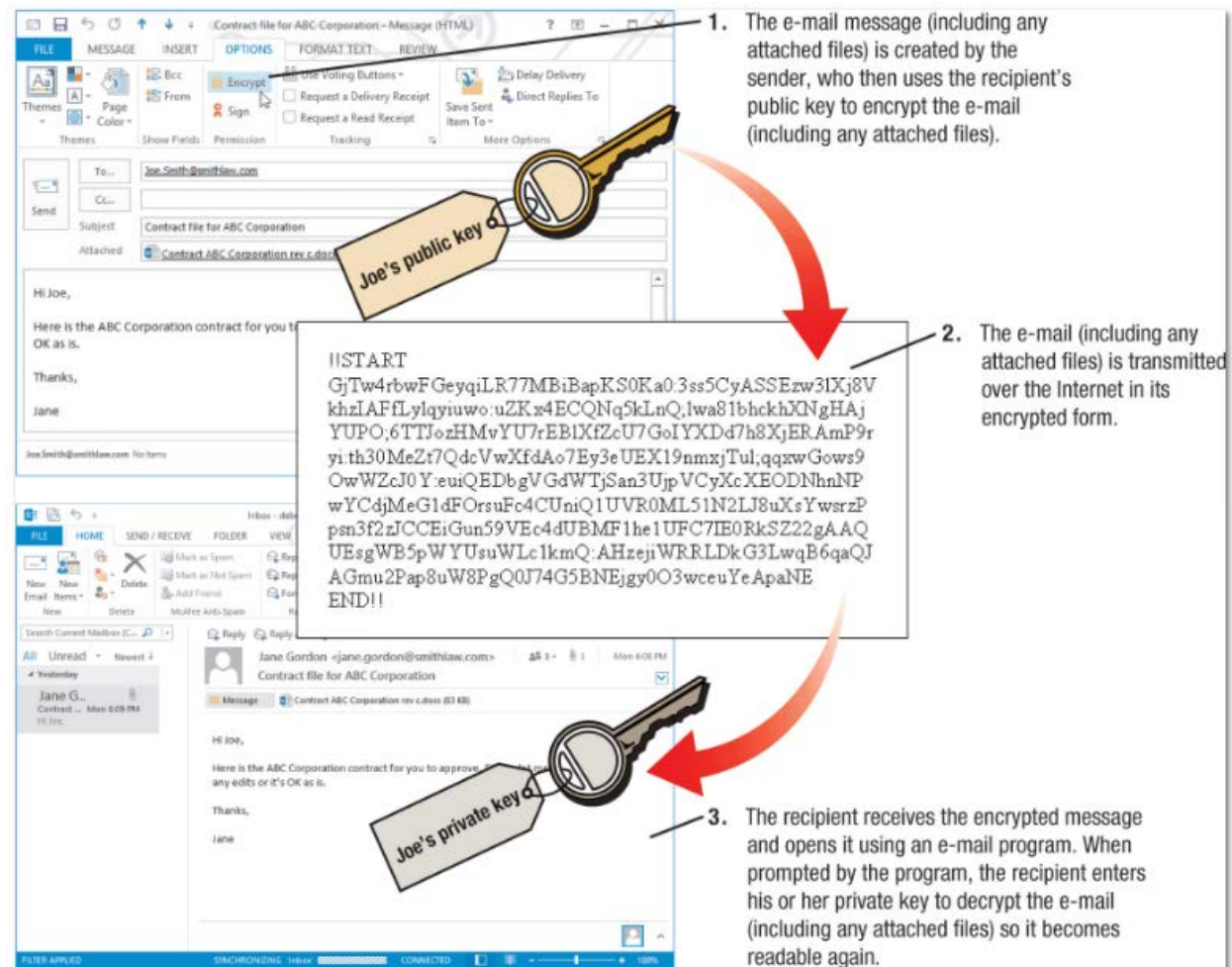


# Types of Encryption

- **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.





# 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



**FIGURE 9-2**

Encrypted devices.

The data on this encrypted USB flash drive cannot be accessed until the user enters the appropriate PIN.



# Access Control

- 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 => something I know

- **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 => something I have

- **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



Source: HID Global Corporation

**FIGURE 9-9**

**Possessed objects.**

Can grant access to both facilities and computing resources.



# Biometric Access Systems => something I am

- **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



# 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.)



# 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



# 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

The screenshot shows the D-Link router configuration interface. Annotations include:

- Use the router's IP address to display the router's configuration screen. (Points to the IP address 192.168.0.1 in the browser address bar)
- Use this tab to enable MAC address filtering. (Points to the TOOLS tab)
- Use this tab to change the administrator password used to access this configuration screen. (Points to the SUPPORT tab)
- Type your desired SSID here. (Points to the Wireless Network Name field)
- Disable SSID broadcast here. (Points to the Enable Auto Channel Scan checkbox)
- Select the desired security mode here. (Points to the Security Mode dropdown menu)
- Type your desired network key here. (Points to the Pre-Shared Key field)

Source: D-Link Systems, Inc.

Configuring a home router.



# 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



# Computer Sabotage

- **Computer sabotage** refers to acts of malicious destruction to a computer or computer resource
  - Launching a malicious program
    - => viruses, worms, Trojans, bots, etc.
  - Altering the content of a Web site
  - Changing data or programs located on a computer



# Botnets

- 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
  - Denial of Service (DoS)



# 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



# 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 Worms

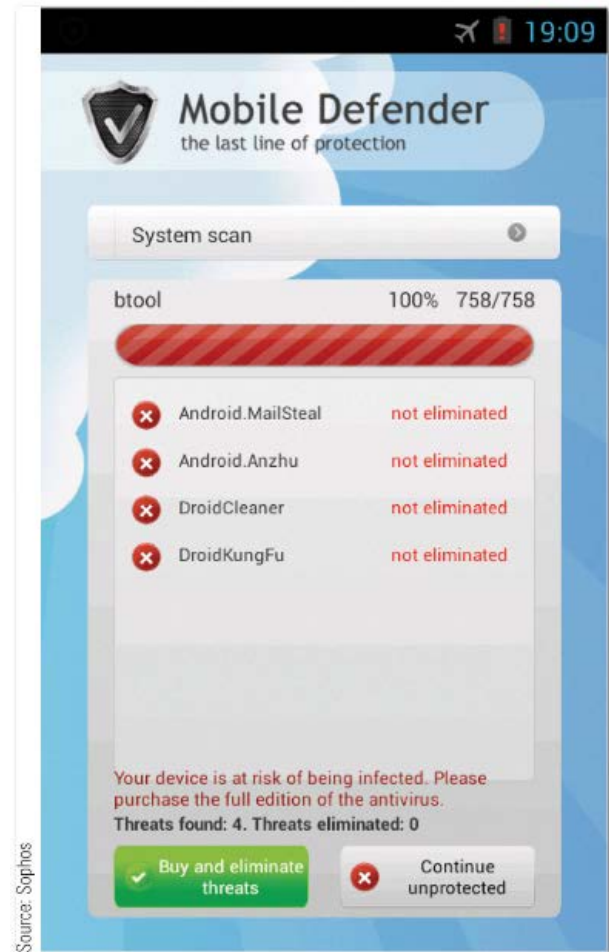
- A **computer virus** is a software program installed without the user's knowledge and designed to alter the way a computer operates or to cause harm to the computer system
  - Often embedded in downloaded programs and e-mail messages (games, videos, music files)
  - Spread when the infected file reaches 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

# 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

**FIGURE 9-17**

**Rogue anti-malware apps.** Try to trick victims into purchasing subscriptions to remove nonexistent malware supposedly installed on their devices.







# Data, Program, or Web Site Alteration

- Hacker can breach 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** 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



# 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
    - => Stateful Packet Inspection (SPI)
  - Important for home computers that have a direct Internet connection, as well as for businesses
  - Work by closing down external communications ports



# Intrusion Prevention Systems

- **Intrusion prevention system (IPS)** software monitors traffic to detect and block possible attacks
  - Help businesses detect and protect against denial of service (DoS) attacks
  - Recommend WiFi logs be turned on



# 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



# 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



# 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 and Other Internet Scams

- **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
  - Check Web browser security settings to prevent programs from being installed without permission, proper cookie setting and information retrieval, etc.
  - 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



# 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

# 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



**FIGURE 9-28**

An anti-cyberbullying Web banner.



# 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



# Aggravated Harassment & Social Computing

- NYS 240.30 - Aggravated harassment in the second degree \*

A person is guilty of aggravated harassment in the second degree when, with intent to harass, annoy, threaten or alarm another person, he or she:

(a) communicates with a person, anonymously or otherwise, by telephone, by telegraph, or by mail, or by transmitting or delivering any other form of written communication, in a manner likely to cause annoyance or alarm;

\*<http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=@SLPEN0P3TNA240+&LIST=LAW+&BROWSER=EXPLORER+&TOKEN=36544786+&TARGET=VIEW>)



# 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



# 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



# 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.

# 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



**FIGURE 9-37**

**Presence technology.** Presence icons indicate the status of individual contacts.



# Protecting Personal Information & Privacy

- 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



# Protecting Personal Information Privacy

- 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



# 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



# 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



# 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



# Network and Internet Security and Privacy Legislation

- Computer security, Internet security, and personal privacy has to 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





# Summary

- 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