15th Edition

Understanding Computers

Today and Tomorrow

Comprehensive

Chapter 15:

Computer Security and Privacy

Deborah Morley
Charles S. Parker

Learning Objectives

1. Explain why all computer users should be concerned about computer security.
2. List some risks associated with hardware loss, hardware damage, and system failure, and understand ways to safeguard a computer against these risks.
3. Define software piracy and digital counterfeiting, and explain how they can be prevented.
4. Explain what information privacy is and why computer users should be concerned about it.

Learning Objectives

5. Describe some privacy concerns regarding databases, electronic profiling, spam, and telemarketing, and identify ways individuals can protect their privacy.
6. Discuss several types of electronic surveillance and monitoring, and list ways individuals can protect their privacy.
7. Discuss the status of computer security and privacy legislation.

Overview

- This chapter covers:
  - Hardware loss, hardware damage, and system failure, and the safeguards that can help reduce the risk of a problem occurring due to these concerns
  - Software piracy and digital counterfeiting and steps that are being taken to prevent these computer crimes
  - Possible risks for personal privacy and precautions that can be taken to safeguard one's privacy
  - Legislation related to computer security and privacy

Why Be Concerned About Computer Security?

- There are a number of security concerns related to computers that users should be concerned about, including:
  - Having a computer or other device stolen
  - Losing important documents
  - Losing a smartphone containing contacts and other important data
  - Buying pirated or counterfeited products

Hardware Loss, Hardware Damage, and System Failure

- Hardware Loss
  - Can occur when a personal computer, USB flash drive, mobile device, or other piece of hardware is stolen, lost, damaged, or experiences a system failure
    - Hardware Theft
      - Most common type of hardware loss
      - Occurs when hardware is stolen from an individual or an organization
      - Often stolen from businesses, schools, and luggage or packages lost by airlines or shipping companies

Hardware Loss, Hardware Damage, and System Failure

  - Often occurs for the value of the hardware, but increasingly for the information that might be contained on the hardware
  - C-level attacks, those targeting CEOs and CIOs, are growing
- Hardware Damage
  - Can occur from power fluctuations, heat, dust, static, electricity, water, and abuse
  - Can be accidental or intentional

Hardware Loss, Hardware Damage, and System Failure

- System Failure and Other Disasters
  - The complete malfunction of a computer system
    - Can be due to a hardware problem, software problem, or computer virus
    - Can be due to a natural disaster or planned attack

Courtesy of Verizon Communications

FIGURE 15-1
System destruction. The 9/11 attacks killed nearly 3,000 people and destroyed hundreds of business offices, including critical cables located in this Verizon office adjacent to Ground Zero.

Hardware Loss, Hardware Damage, and System Failure

- Protecting Against Hardware Loss, Hardware Damage, and System Failure
  - Door and Computer Equipment Locks
    - Prevent access to equipment
    - Cable locks, security slots, cable anchors
    - Security cases
    - Laptop alarm software
    - Lock up USB flash drives, external hard drives, and other media
    - Businesses can run social engineering tests to assess the vulnerability of their facility and employees

Hardware Loss, Hardware Damage, and System Failure

Courtesy of Kensington Computer Products Group

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.

FIGURE 15-3
Cable locks secure computers and other hardware.

Trend Box

Self-Healing Devices

- Repair themselves when damaged
- New plastic that mimics our skin's ability to repair itself
  - Turns red until it reforms
- Special paint that can repair scratches or cuts
  - Scratch Shield iPhone case

This Scratch Shield case from Nissan can repair itself when scratched.

Hardware Loss, Hardware Damage, and System Failure

- Encryption and Self-Encrypting Hard Drives
  - Use encryption to protect data
  - Increasingly used with USB flash drives, portable computers, smartphones, etc.
  - Full Disk Encryption (FDE)
    - Everything on the storage medium is encrypted
  - Self-Encrypting Hard Drive
    - A hard drive using FDE
    - Used most often with portable computers

FIGURE 15-4
Encrypted devices. The data on this encrypted USB flash drive cannot be accessed until the user enters the appropriate PIN.

Hardware Loss, Hardware Damage, and System Failure

- Device Tracking Software and Antitheft Tools
  - Used to find a computer or other device after it is lost or stolen
  - Sends out identifying data via the Internet
  - Law enforcement can use this data to recover the device
  - Kill Switch
    - Causes the device to self-destruct
  - Asset Tags (permanently attached)
  - Tamper Evident Labels
    - Change their appearance if someone tries to remove them

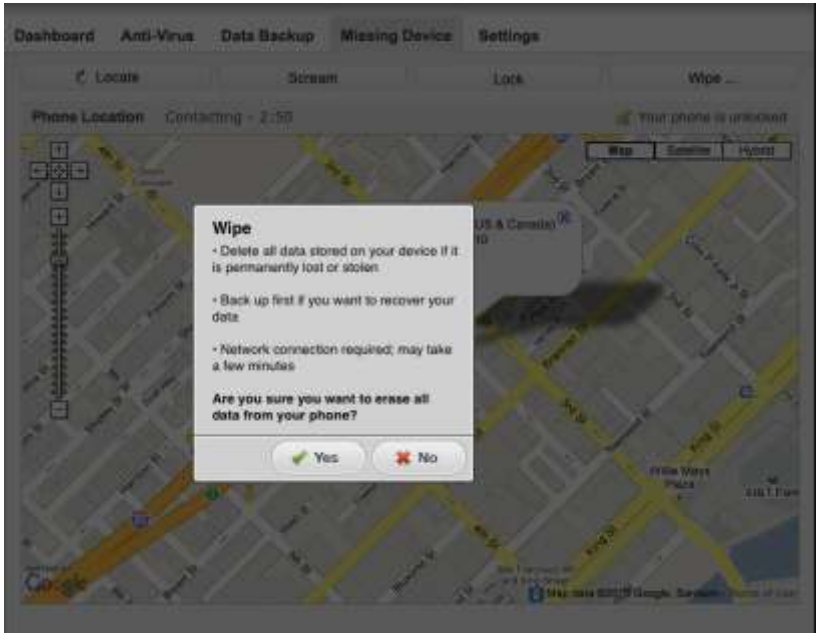
Courtesy Bullguard

FIGURE 15-5
Device tracking software.

How It Works Box

Self-Destructing Devices

- Contain a kill switch that can be used to destroy the device or data stored on it to prevent access
- Activated by the customer or a tracking company upon customer request
- Activated when the device accesses the Internet or when a remote trigger (like a number of logon attempts) is activated
- Can be used with some cloud services



Hardware Loss, Hardware Damage, and System Failure

- Additional Precautions for Mobile Users
  - Mobile Device Management (MDM) software
    - Used by businesses to manage mobile devices used by employees
    - Locks down or wipes a lost or stolen phone
    - Displays a message with instructions for returning the device
    - Displays the current location of the device
  - Wireless Tether System
    - Ties phone to a key fob in order to sound an alarm and lock the phone if further away than the specified allowable distance

Hardware Loss, Hardware Damage, and System Failure

- Use common sense and do not leave personal computers and mobile devices unattended
- Use cloud services so data will not be stored on your devices
- Disable wireless connections when they are not needed

MOBILE COMPUTING PRECAUTIONS
Install and use encryption, antivirus, antispyware, and firewall software.
Secure computers with boot passwords; set your mobile phone to autolock the screen after a short period of time and require a passcode to unlock it.
Use only secure Wi-Fi connections and disable Wi-Fi and Bluetooth when they are not needed.
Never leave usernames, passwords, or other data attached to your computer or inside its carrying case.
Use a plain carrying case to make a portable computer less conspicuous.
Keep an eye on your devices at all times, especially when going through airport security.
Avoid setting your devices on the floor or leaving them in your hotel room; use a cable lock to secure the device to a desk or other object whenever this is unavoidable.
Back up the data stored on the device regularly, but don't carry the backup media with your device and don't store unencrypted sensitive data on your device.
Consider installing tracking or kill switch software.

FIGURE 15-6
Common-sense precautions for portable computer and mobile device users.

Hardware Loss, Hardware Damage, and System Failure

- Proper Hardware Care
  - Do not harm hardware physically
  - Use protective cases

FIGURE 15-7
Protective cases.

Hardware Loss, Hardware Damage, and System Failure

- Ruggedized devices are available
  - Designed to withstand much more physical abuse than conventional computers

RUGGED LAPTOPS

RUGGED TABLETS

RUGGED PHONES

FIGURE 15-8
Ruggedized devices.

Hardware Loss, Hardware Damage, and System Failure

- Use surge suppressors
- Use uninterruptible power supplies (UPSs)
  - Provide continuous power to a computer system after the power goes off
- Avoid exposing devices to dust, moisture, static, and heat
- Avoid a head crash
- Stop USB devices before removing them
- Use screen protectors, jewel cases, etc.

Hardware Loss, Hardware Damage, and System Failure

Courtesy of Schneider Electric

SURGE SUPPRESSOR

UPS

FIGURE 15-9
Surge suppressors and uninterruptible power supplies (UPSs).

FIGURE 15-10
Proper hardware care. Unless your computer is ruggedized (such as the one shown here), keep it out of the heat, cold, rain, water, and other adverse conditions.

Courtesy General Dynamics Itronix

Hardware Loss, Hardware Damage, and System Failure

- Backups and Disaster Recovery Plans
  - Essential for both businesses and individuals
  - Backup media needs to be secured
    - Data storage companies store backup media at secure remote locations
    - Online backup is another possibility
  - Continuous data protection (CDP)
    - Enables data backups to be made on a continual basis
  - Disaster-recovery plan
    - Describes the steps a company will take following the occurrence of a disaster
    - Hot site can be used in facilities are destroyed
    - Emergency or Web-based mail provider

Technology and You Box

Protecting Your PC

- Step 1: Protect your hardware.
- Step 2: Install and use security software.
- Step 3: Back up regularly.
- Step 4: Update your operating system, browser, and e-mail program regularly.
- Step 5: Test your system for vulnerabilities.

Continuous data protection (CDP) protects your data on an ongoing basis.

Quick Quiz

1. Which of the following would not likely be a reason for stealing a notebook computer?
   a. For the data contained on the computer
   b. To use in a denial of service (DoS) attack
   c. For the value of the hardware
2. True or False: It is only important to use a surge suppressor during bad weather, when a lightning strike may occur.
3. A copy of a file that is created in case the original is damaged is called a(n) _____.

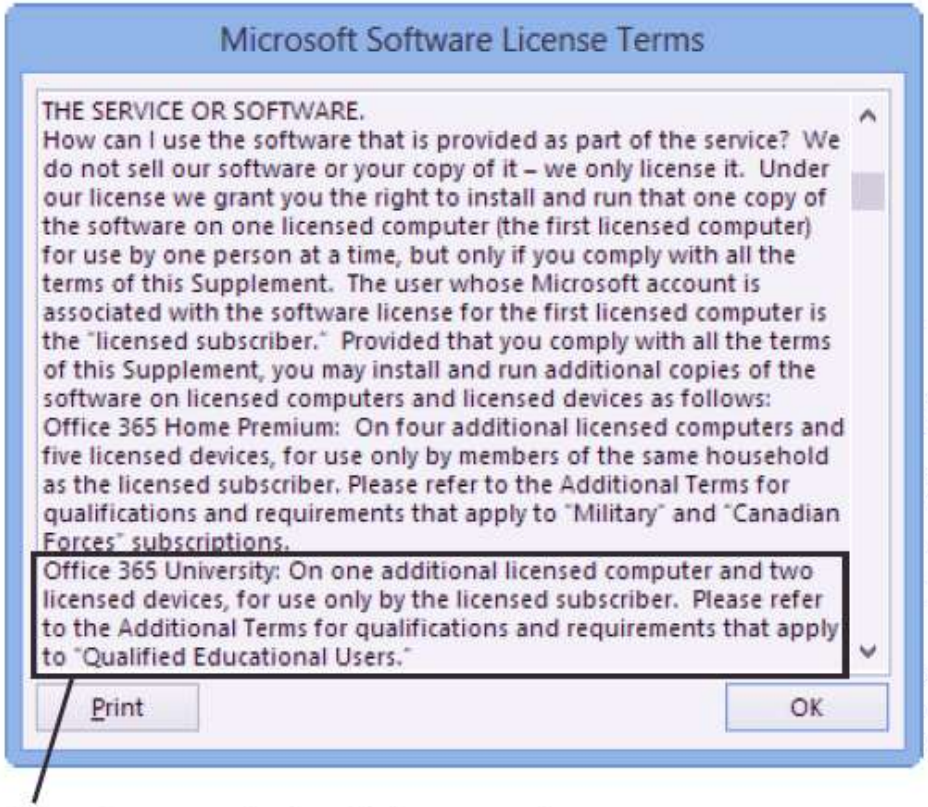
Answers:

1) b; 2) False; 3) backup

Software Piracy and Digital Counterfeiting

- Software Piracy
  - Unauthorized copying of a computer program occurs when:
    - Individuals make illegal copies of software to give to friends
    - Businesses or individuals install software on more than the number of computers allowed according to the end-user license agreement (EULA)
    - Sellers install unlicensed copies on computers sold to consumers
    - Large-scale operations in which programs and packaging are illegally duplicated and sold as supposedly legitimate products

Software Piracy and Digital Counterfeiting



Used with permission from Microsoft Corporation

FIGURE 15-11

An end-user license agreement (EULA). Specifies the number of computers on which the software can be installed and other restrictions for use.

Software Piracy and Digital Counterfeiting

- Digital Counterfeiting
  - The use of computers or other types of digital equipment to make illegal copies of documents
    - Currency, checks, collectibles and other items
    - Often scanned and printed or color-copied
  - Illegal in the United States

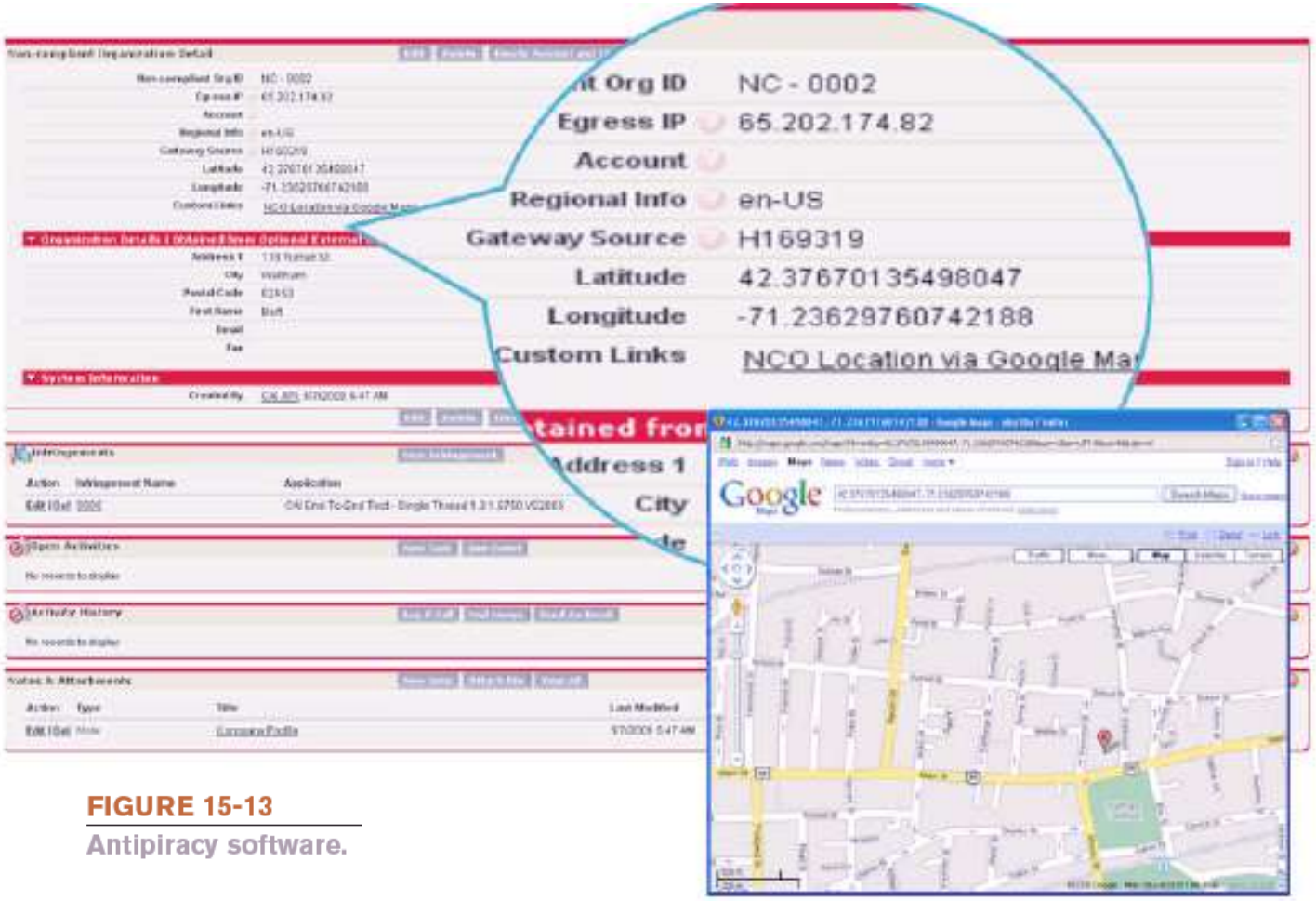
Courtesy of United States Secret Service

FIGURE 15-12
Digitally counterfeited documents.

Software Piracy and Digital Counterfeiting

- Protecting Against Software Piracy and Digital Counterfeiting
  - Software Antipiracy Tools
    - Educating businesses and consumers
    - Requiring a unique registration code or product key
    - Checking validity of a software installation before upgrades or other resources related to the program can be used
    - Watching online auction sites and requesting removal of suspicious items
    - Incorporating code into applications to inform the vendor when pirated copies are being used, or are in violation of the license

Software Piracy and Digital Counterfeiting



Courtesy Vi Labs; Google screenshot © Google Inc. and used with permission.

FIGURE 15-13
Antipiracy software.

Software Piracy and Digital Counterfeiting

- Digital Counterfeiting Prevention
  - New currency designs released every seven to ten years by the U.S. Treasury Department
    - Microprinting, watermarks, a security thread, color-shifting ink, and raised printing are used
  - Digital watermarks and RFID tags can also be used to deter counterfeiting checks and ID cards
    - Digital watermark
      - » Subtle alteration to a digital item that is not noticeable but that can be retrieved to identify the owner of the item

Software Piracy and Digital Counterfeiting

Photo courtesy of United States Secret Service

FIGURE 15-14
Anticounterfeiting measures used with U.S. currency.

Quick Quiz

1. Using a computer to make illegal copies of currency to circulate as real currency is a form of _____.
   a. software piracy
   b. computer sabotage
   c. digital counterfeiting
2. True or False: Software piracy is rarely performed today.
3. The use of computers or other types of digital equipment to make illegal copies of currency, checks, collectibles, and other items is known as _____.

Answers:

1) c; 2) False; 3) digital counterfeiting

Why Be Concerned About Information Privacy?

- Privacy
  - State of being concealed or free from unauthorized intrusion
- Information Privacy
  - Rights of individuals and companies to control how information about them is collected and used
- Computers add additional privacy challenges
  - Cookies and spyware are possible privacy risks
  - Databases, spam, electronic surveillance, electronic monitoring present additional privacy concerns

Databases, Electronic Profiling, Spam, and Other Marketing Activities

- Databases and Electronic Profiling
  - Unless data stored in databases is sufficiently protected, security breaches can occur
  - Marketing databases, government databases, and educational databases are at higher risk for personal privacy violations
    - Marketing Databases
      - Collection of marketing and demographic data about people and used for marketing purposes
      - Data obtained through online and offline purchases, public information, etc.

Databases, Electronic Profiling, Spam, and Other Marketing Activities

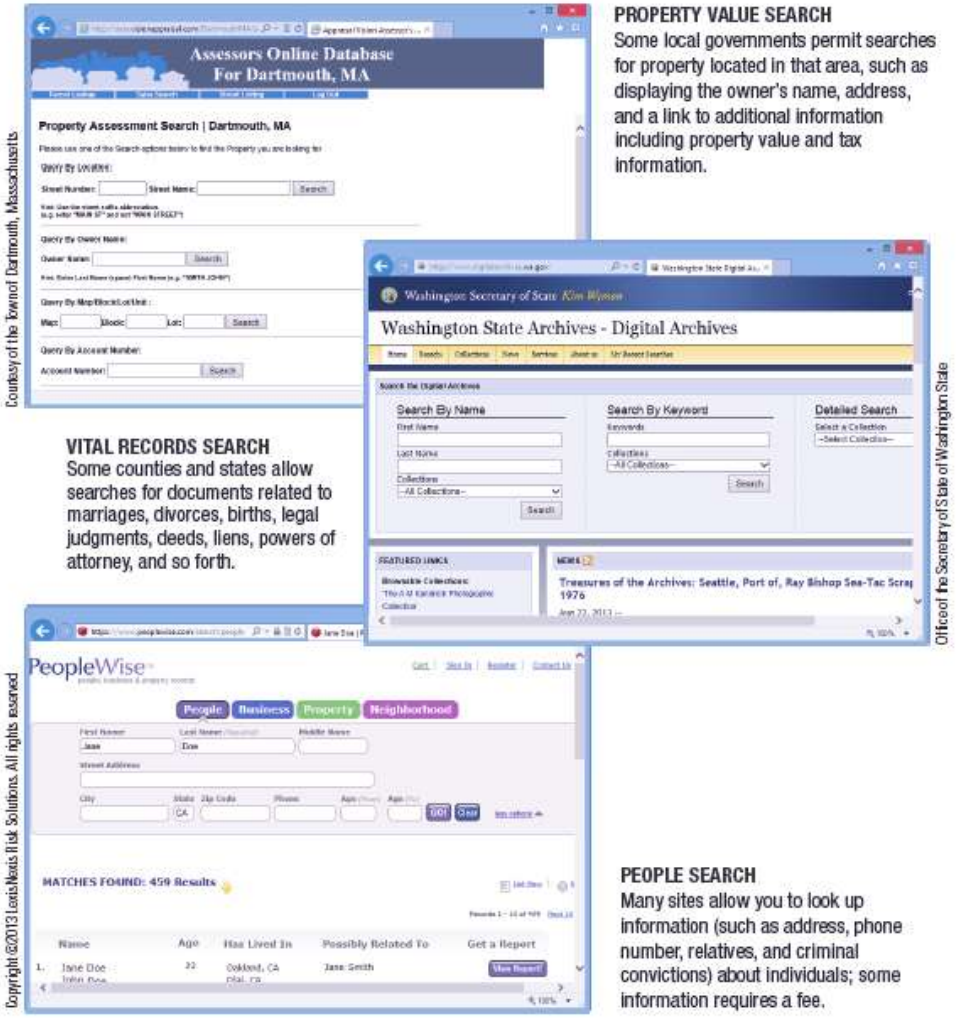
- Data is also gathered from Web and social media activities
  - » Facebook, MySpace, Google+, and location services such as Foursquare

- Government Databases
  - Collection of data about people, collected and maintained by the government
  - Some information is confidential, other is public
    - » Tax information, and Social Security earnings are private
    - » Birth records, marriage, and divorce information are public

Databases, Electronic Profiling, Spam, and Other Marketing Activities

- Real ID Act of 2005
  - » Mandates the development of a national ID system that links driver's license databases across the country
- The emerging Federal Services Data Hub database
  - » Will be used to connect healthcare insurance exchanges with numerous federal databases
- Much information about an individual is available for free on the Internet

Databases, Electronic Profiling, Spam, and Other Marketing Activities



PROPERTY VALUE SEARCH
Some local governments permit searches for property located in that area, such as displaying the owner's name, address, and a link to additional information including property value and tax information.

VITAL RECORDS SEARCH
Some counties and states allow searches for documents related to marriages, divorces, births, legal judgments, deeds, liens, powers of attorney, and so forth.

PEOPLE SEARCH
Many sites allow you to look up information (such as address, phone number, relatives, and criminal convictions) about individuals; some information requires a fee.

FIGURE 15-15
A variety of searchable databases are available via the Internet.

Databases, Electronic Profiling, Spam, and Other Marketing Activities

- Electronic Profiling
  - Using electronic means to collect a variety of in-depth information about an individual
  - Designed to provide specific information which is then sold to companies to be used for marketing purposes

When you make an electronic transaction, information about who you are and what you buy is recorded, usually in a database.

Databases containing the identities of people and what they buy are sold to marketing companies.

The marketing companies add the new data to their marketing databases; they can then reorganize the data in ways that might be valuable to other companies.

The marketing companies create lists of individuals matching the specific needs of companies; the companies buy the lists for their own marketing purposes.

FIGURE 15-16
How electronic profiling might work.

Databases, Electronic Profiling, Spam, and Other Marketing Activities

- Privacy Policy
  - Included on many Web sites
  - Dictates how supplied information will be used, but can be changed and often without notice

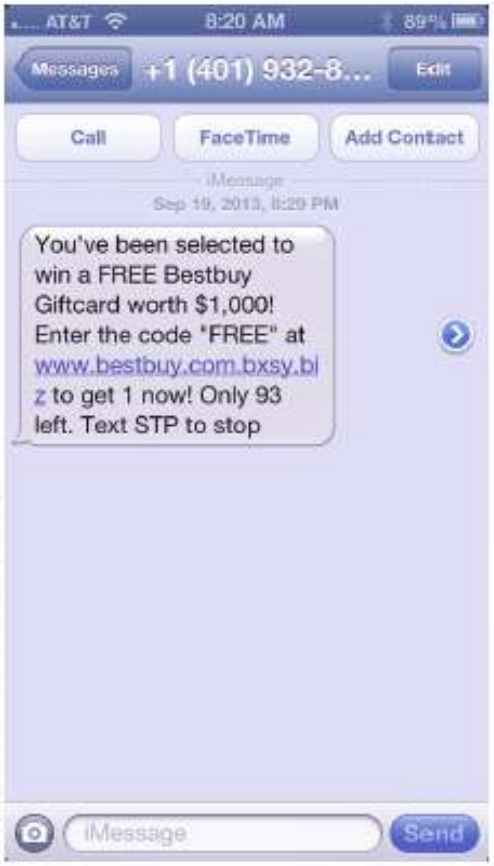
FIGURE 15-17
Privacy policies. Web site privacy policies explain how your personal information might be used.

Databases, Electronic Profiling, Spam, and Other Marketing Activities

- Spam and Other Marketing Activities
  - Unsolicited, bulk e-mail sent over the Internet
  - Often involves health-related products, counterfeit products, fraudulent business opportunities, pornography, etc.
  - Marketing e-mails from companies a person has done business with
  - Can be delivered via instant messaging (spim), text messages (mobile phone or SMS spam), social networking sites, phones, and fax machines
  - Wastes time, bandwidth, and productivity
  - CAN-SPAM Act of 2003 enacted some requirements and penalties for commercial e-mailers

Databases, Electronic Profiling, Spam, and Other Marketing Activities

E-MAIL SPAM



TEXT MESSAGE SPAM

FIGURE 15-18
Examples of spam.

Protecting the Privacy of Personal Information

- Safeguard Your E-Mail Address
  - Use one private e-mail address for trusted sources likes friends, family, and colleagues
  - Use a throw-away (disposable) e-mail address for online shopping, forums, product registration, sweepstakes, etc.

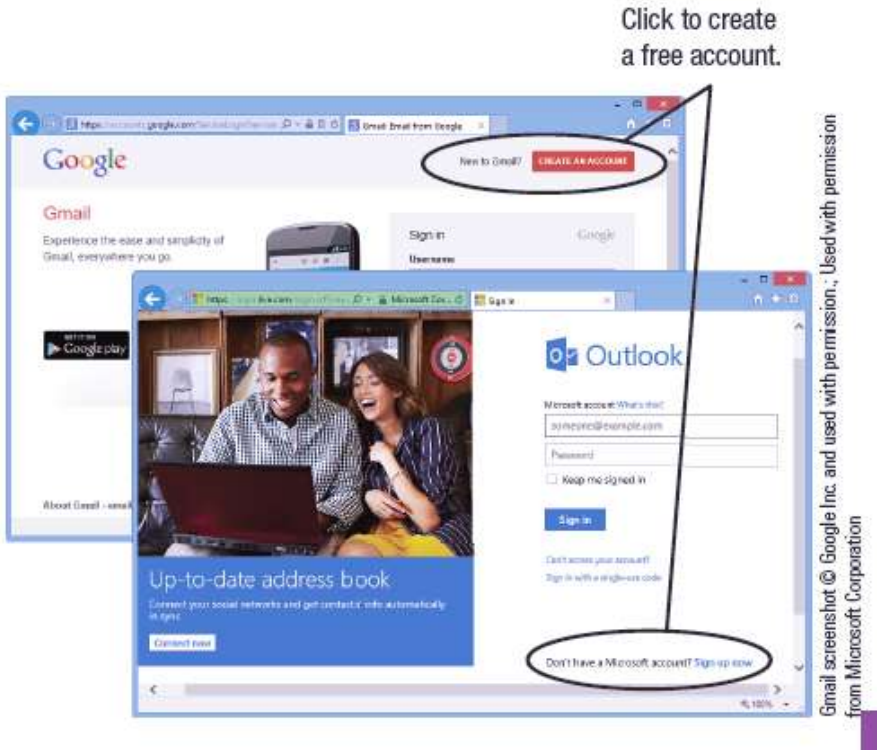


FIGURE 15-19
Free e-mail accounts. Can be used for throw-away e-mail addresses.

Protecting the Privacy of Personal Information

- Be Cautious of Revealing Personal Information
  - Read a Web site's privacy policy
  - Avoid putting too many personal details on your Web sites and social media pages; restrict access to friends and family
  - Use a throw-away email address when signing up for free trials or other services than may result in spam
  - Consider using privacy software, such as Privacy Guardian to hide personal information while browsing the Web
  - Supply only the required information in registration forms
  - Delete your browsing history and e-mail settings when using a public computer; use private browsing

Protecting the Privacy of Personal Information

Facebook (use Privacy Settings)	Limit who can see your posts to *Friends* only. Limit who can look you up to *Friends* or *Friends of Friends* only. Disable search engines linking to your timeline. If you allow friends to post on your timeline, enable the settings to review the posts first. On your profile's *About* page, click each section and limit viewing to *Friends* only.
Google+ (use Profile Settings)	Organize your contacts into *circles* based on the content you will share with them (such as work, friends, and family) and then post or share content only with the appropriate circle. On your profile's *About* page, click each section and limit viewing to *Your circles* only.
Twitter (use Account Settings)	Enable *Tweet privacy* so only those who you approve will receive your tweets. Keep location information disabled so your location won't be added to your tweets.

FIGURE 15-20
Social media privacy tips.

Protecting the Privacy of Personal Information

- Use Filters and Opt Out
  - Use an e-mail filter to automatically sort e-mail messages and route possible spam into a special folder to deal with later
  - Be sure to check spam folders for important messages
  - Spam filters can be used to catch spam
    - Mobile spam apps can be used with mobile devices

© Chanchai n/Shutterstock.com; Courtesy Numbercop

FIGURE 15-23
Mobile spam filtering. Can detect both spam texts and spam calls.

Protecting the Privacy of Personal Information

- Opt out of marketing activities
  - Request to be removed from marketing lists or that personal information not be shared with other companies
  - Can contact companies directly
  - Opt-out tools are available online
  - Opt-out cookies prevent marketing cookies from being stored on your computer
  - Some privacy groups want individuals to have to opt in to activities instead
  - Proposed Do Not Track legislation

Protecting the Privacy of Personal Information

- Can enable tracking protection in browsers

Used with permission from Microsoft Corporation

FIGURE 15-24
Enabling tracking protection in Internet Explorer.

Protecting the Privacy of Personal Information

- Secure Servers and Otherwise Protect Personal Information
  - Automatic encryption systems for e-mail can help sensitive data from accidentally being revealed
  - Chief Privacy Officer (CPO)
    - Ensures that the private data stored by businesses is adequately protected
    - Ensures privacy laws are complied with
    - Identifies the data in a company that needs to be protected
    - Develops policies to protect the data

Protecting the Privacy of Personal Information

- Properly Dispose of Hardware Containing Data
  - Wipe (not just delete) data on hard drives before disposing of a computer or hard drive
  - Storage media containing sensitive data should be shredded
  - Businesses should have a media sanitation/data destruction policy

Courtesy Fellowes, Inc.

FIGURE 15-25
Media disposal. When disposing of CDs, DVDs, and other storage media, the media should be shredded to ensure the information on the media is destroyed.

Inside the Industry Box

- Data Killers
  - Data destruction services can be used to destroy data contained on storage media
  - Magnetic hard drives can be wiped or degaussed (demagnetized)
  - Other media can be shredded
  - Method depends on the type of media and where the hardware is going

Hard drive before (left) and after (right) shredding.

Electronic Surveillance and Monitoring

- Computer Monitoring Software
  - Records an individual's computer usage by capturing images of the screen, recording the actual keystrokes used, or creating a summary of Web sites visited
  - Can be used in homes by adults to monitor computer usage of children or spouse
  - Can be used in businesses to monitor employee computer usage
  - Also used by government agencies
  - Keystroke-logging systems
    - Used to capture keystrokes
    - Can be used by hacker to capture usernames, passwords, and other sensitive information entered into a computer via the keyboard

Electronic Surveillance and Monitoring

FIGURE 15-26
Computer monitoring software. Can be used to monitor employee computer activity, as shown here.

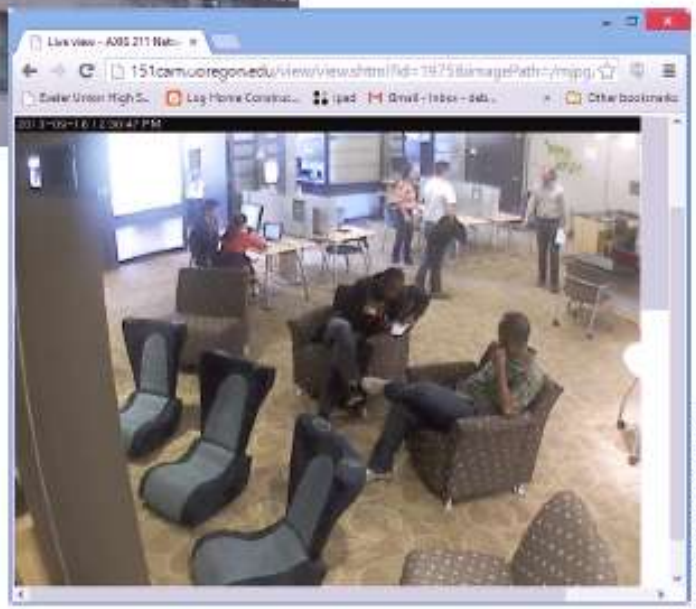
Electronic Surveillance and Monitoring

- Video Surveillance
  - The use of video cameras to monitor activities of individuals
  - Used to monitor employees
  - Used in public locations for law enforcement purposes
    - Stores and other businesses, public streets, subways, airports, etc.
  - Can be used with face recognition software
    - Identify terrorists and other known criminals
  - Privacy advocates object to the use of video surveillance and face recognition technology in public places
  - Privacy concerns also exist regarding digital cameras capabilities in smartphones, Google Glass, etc.

Electronic Surveillance and Monitoring

Image source: EFF.org project Observing Surveillance

OUTDOOR SURVEILLANCE
Many cameras placed in public locations are designed to blend into their surroundings to be less intrusive, such as the camera inside this light fixture on a Washington, D.C., street.



INDOOR SURVEILLANCE
Many cameras are placed inside businesses, schools, and other locations; a snapshot from a video camera located at a university in Oregon is shown here.

Courtesy University of Oregon

FIGURE 15-27
Examples of public video surveillance.

Electronic Surveillance and Monitoring

- Employee Monitoring
  - Observing or recording employees' actions while they are on the job; legal and quite common
  - Can monitor computer usage, phone calls, e-mail, etc.
  - To monitor physical location, use
    - Video cameras
    - GPS monitoring systems
    - Proximity cards and apps
      - Can be used for access control
    - Businesses should inform employees

FIGURE 15-29
Proximity apps.
This app locks and unlocks your computer automatically as your iPhone moves in and out of range.

Electronic Surveillance and Monitoring

- Presence Technology
  - Enables one computing device on a network to locate and identify the current status of another device on the same network
  - Can tell if a someone is using his/her computer or mobile phone
  - Built into IM and some social networking sites
  - May also be used for marketing activities in the future
  - Potential privacy concerns

FIGURE 15-30
Presence technology. Presence icons indicate the status of individual contacts.

Electronic Surveillance and Monitoring

- Protecting Personal and Workspace Privacy
  - Can use antispyware software to detect and remove some types of illegal computer monitoring and spyware software
  - The Employer's Responsibilities
    - Keep employee, company, and customer information private and secure
    - Monitor employees' activities to ensure they are productive
    - Have an employee policy that informs employees about company's monitoring activities

Electronic Surveillance and Monitoring

- The Employees' Responsibilities
  - Read the company's employee policy and review it periodically to ensure
  - Do not violate any company rules
  - Avoid personal activities at work
  - Sending jokes via e-mail to coworkers might be interpreted as harassment

Computer Security and Privacy Legislation

- A variety of laws have been passed since the 1970s due to the high level of concern about computer security and personal privacy
  - Congress has had difficulty passing new legislation because
    - It is difficult for legal system to keep pace with technology changes
    - Privacy is difficult to define and there is a struggle to balance freedom of speech with the right to privacy
    - Recent proposed actions
      - Do-Not-Track Online Act of 2013
      - Consumer Privacy Bill or Rights

Computer Security and Privacy Legislation

DATE	LAW AND DESCRIPTION
2009	**American Recovery and Reinvestment Act** Requires HIPAA covered entities to notify patients and/or customers when protected health information has been compromised.
2006	**U.S. SAFE WEB Act of 2006** Grants additional authority to the FTC to help protect consumers from spam, spyware, and Internet fraud and deception.
2005	**Real ID Act** Establishes national standards for state-issued driver's licenses and identification cards.
2005	**Junk Fax Prevention Act** Requires unsolicited faxes to have a highly visible opt-out notice.
2003	**CAN-SPAM Act** Implements regulations for unsolicited e-mail messages and lays the groundwork for a federal Do Not E-Mail Registry.
2003	**Do Not Call Implementation Act** Amends the Telephone Consumer Protection Act to implement the National Do Not Call Registry.
2003	**Health Insurance Portability and Accountability Act (HIPAA)** Includes a Security Rule that sets minimum security standards to protect health information stored electronically.
2002	**Sarbanes-Oxley Act** Requires archiving a variety of electronic records and protecting the integrity of corporate financial data.
2001	**USA PATRIOT Act** Grants federal authorities expanded surveillance and intelligence-gathering powers, such as broadening the ability of federal agents to obtain the real identity of Internet users and to intercept e-mail and other types of Internet communications.

FIGURE 15-31
Federal legislation related to computer security and privacy.

Computer Security and Privacy Legislation

1999	**Financial Modernization (Gramm-Leach-Bliley) Act** Extends the ability of banks, securities firms, and insurance companies to share consumers' non-public personal information, but requires them to notify consumers and give them the opportunity to opt out before disclosing any information.
1998	**Child Online Protection Act (COPA)** Prohibits online pornography and other content deemed harmful to minors; has been blocked by the Supreme Court.
1998	**Children's Online Privacy Protection Act (COPPA)** Regulates how Web sites can collect information from minors and communicate with them.
1998	**Telephone Anti-Spamming Amendments Act** Applies restrictions to unsolicited, bulk commercial e-mail.
1991	**Telephone Consumer Protection Act** Requires telemarketing companies to respect the rights of people who do not want to be called.
1988	**Computer Matching and Privacy Protection Act** Limits the use of government data in determining federal-benefit recipients.
1988	**Video Privacy Protection Act** Limits disclosure of customer information by video-rental companies.
1986	**Electronic Communications Privacy Act** Extends traditional privacy protections governing postal delivery and telephone services to include e-mail, mobile phones, and voice mail.
1984	**Cable Communications Policy Act** Limits disclosure of customer records by cable TV companies; extended in 1992 to include companies that sell wireless services.
1974	**Education Privacy Act** Stipulates that, in both public and private schools that receive any federal funding, individuals have the right to keep the schools from releasing information such as grades and evaluations of behavior.
1974	**Privacy Act** Stipulates that the collection of data by federal agencies must have a legitimate purpose.
1970	**Fair Credit Reporting Act** Prevents private organizations from unfairly denying credit and provides individuals the right to inspect their credit records.
1970	**Freedom of Information Act** Gives individuals the right to inspect data concerning them that is stored by the federal government.

FIGURE 15-31
Federal legislation related to computer security and privacy.

Quick Quiz

1. A document that discloses how your personal information will be used is called a(n) _____.
   a. privacy policy
   b. opt out
   c. throw-away e-mail address
2. True or False: The problem of protecting personal privacy and keeping personal information private did not exist before computers and the Internet.
3. The ability of one computing device on a network to identity the status of another device on that network is known as _____.

Answers:

1) a; 2) False; 3) presence technology

Summary

- Why Be Concerned About Computer Security?
- Hardware Loss, Hardware Damage, and System Failure
- Software Piracy and Digital Counterfeiting
- Why Be Concerned About Information Privacy?
- Databases, Electronic Profiling, Spam, and Other Marketing Activities
- Electronic Surveillance and Monitoring
- Computer Security and Privacy Legislation