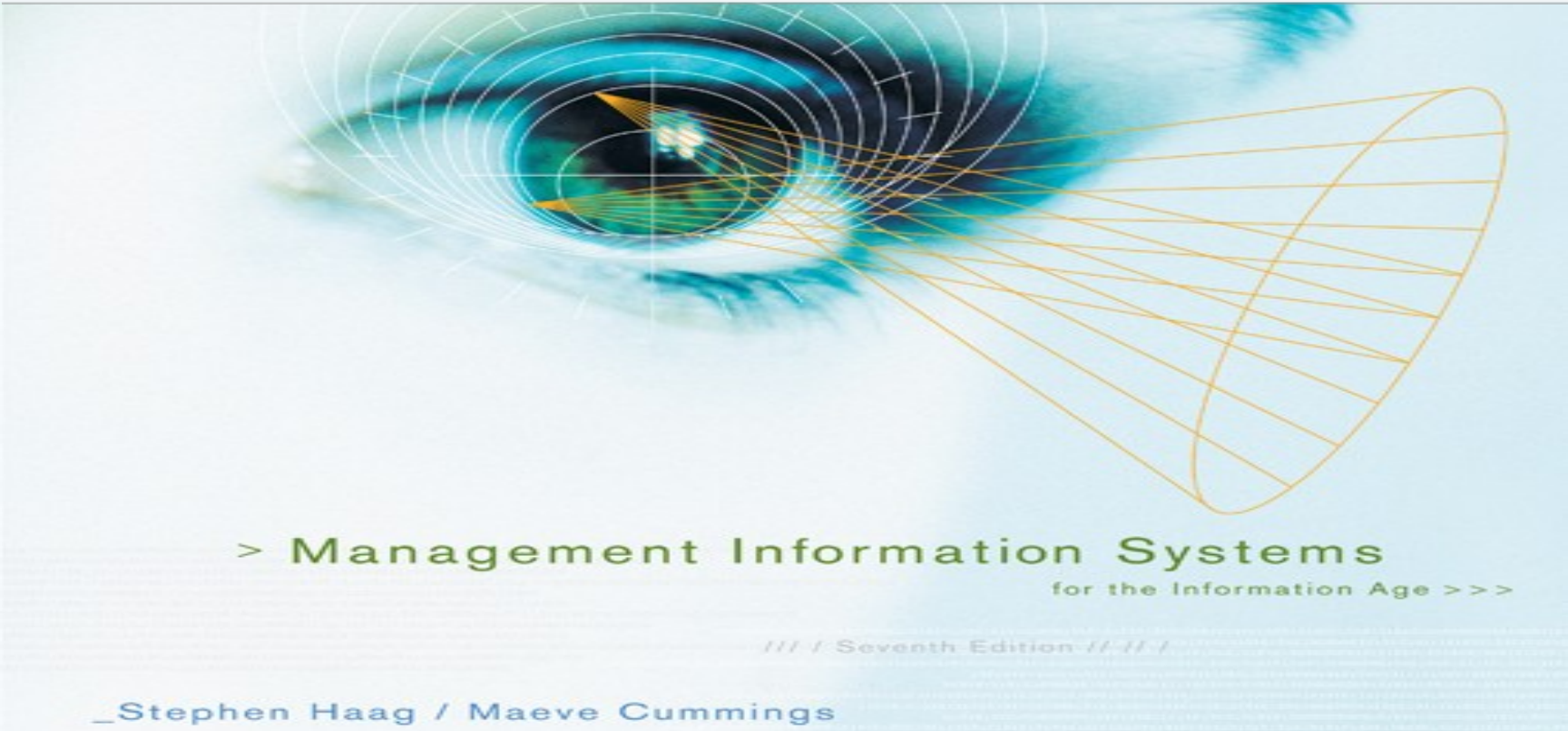
# Chapter 8
# PROTECTING PEOPLE AND INFORMATION
## Threats and Safeguards



# STUDENT LEARNING OUTCOMES

1. Define ethics and describe the two factors that affect how you make a decision concerning an ethical issue.
2. Define and describe intellectual property, copyright, Fair Use Doctrine, and pirated software.
3. Describe privacy and describe ways in which it can be threatened.
4. Describe the ways in which information on your computer or network is vulnerable and list measures you can take to protect it.

# THEY KNOW ABOUT 96% OF AMERICAN HOUSEHOLDS

- Customers: 9 of the 10 largest credit-card issuers
- Acxiom has 20 billion records on
  - 110 million people
  - 96% of households
- Makes and sells lists to customers
- Merges and protects databases

# Case Study Questions

1. Do you feel comfortable about so many people collecting information about you and distributing it freely?
2. Is it an invasion of your privacy or just good business?
3. Should there be any laws regulating the collection and use of data by data brokers like Acxiom?

# INTRODUCTION

- Handling information responsibly means understanding the following issues
  - Ethics
  - Personal privacy
  - Threats to information
  - Protection of information

# CHAPTER ORGANIZATION

1. Ethics
   - Learning Outcomes #1 & #2
2. Privacy
   - Learning Outcome #3
3. Security
   - Learning Outcome #4

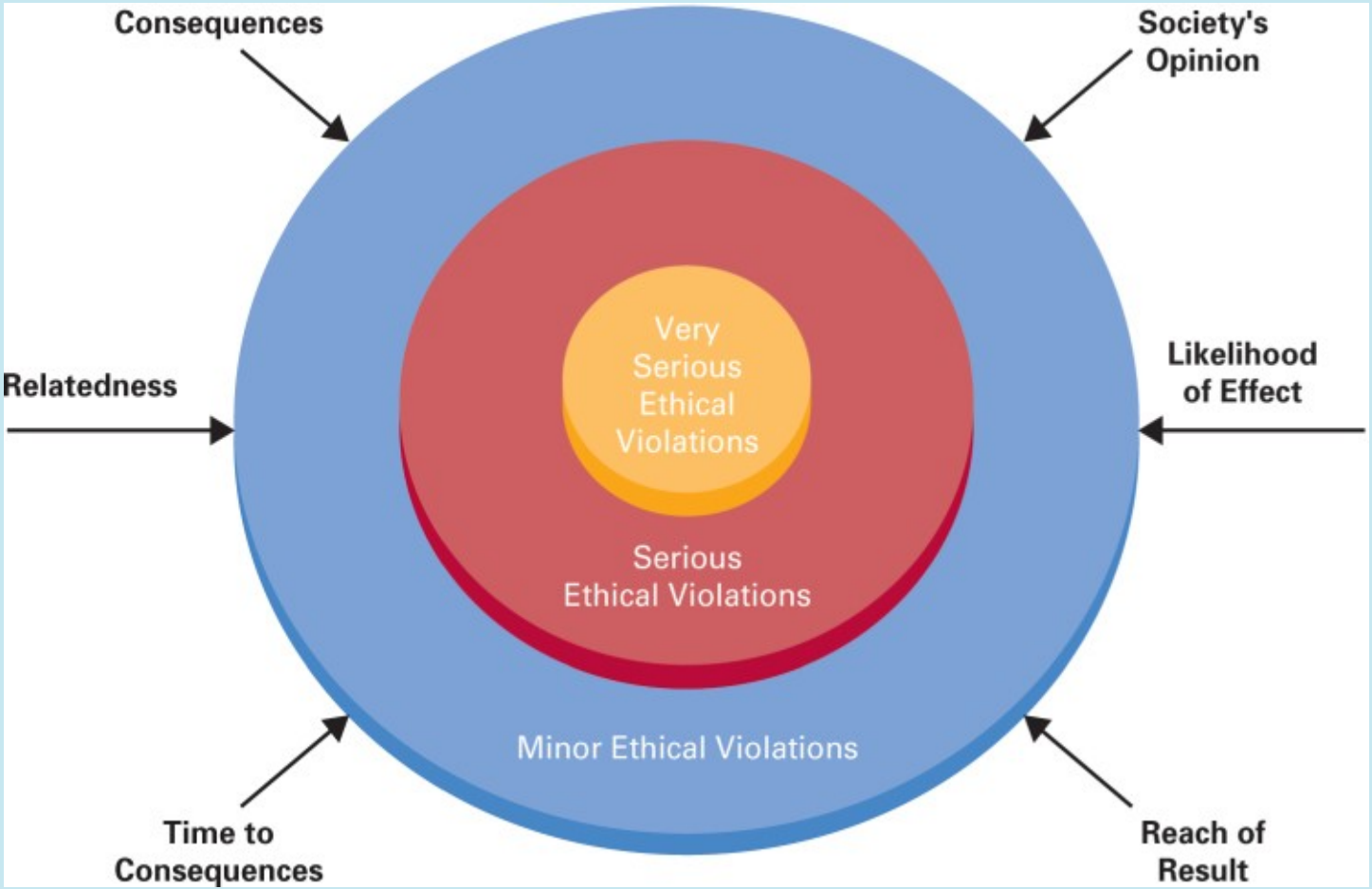
# ETHICS

- ***Ethics*** – the principles and standards that guide our behavior toward other people
- Ethics are rooted in history, culture, and religion

# Factors the Determine How You Decide Ethical Issues

- Actions in ethical dilemmas determined by
  - Your basic ethical structure
  - The circumstances of the situation
- Your basic ethical structure determines what you consider to be
  - Minor ethical violations
  - Serious ethical violations
  - Very serious ethical violations

# Basic Ethical Structure



# Circumstances of the Situation

1. Consequences of the action or inaction
2. Society's opinion of the action or inaction
3. Likelihood of effect of action or inaction
4. Time to consequences of action or inaction
5. Relatedness of people who will be affected by action or inaction
6. Reach of result of action or inaction

# Intellectual Property

- ***Intellectual property*** – intangible creative work that is embodied in physical form
- ***Copyright*** – legal protection afforded an expression of an idea
- ***Fair Use Doctrine*** – may use copyrighted material in certain situations

# Intellectual Property

- Using copyrighted software without permission violates copyright law
- ***Pirated software*** – the unauthorized use, duplication, distribution, or sale of copyrighted software

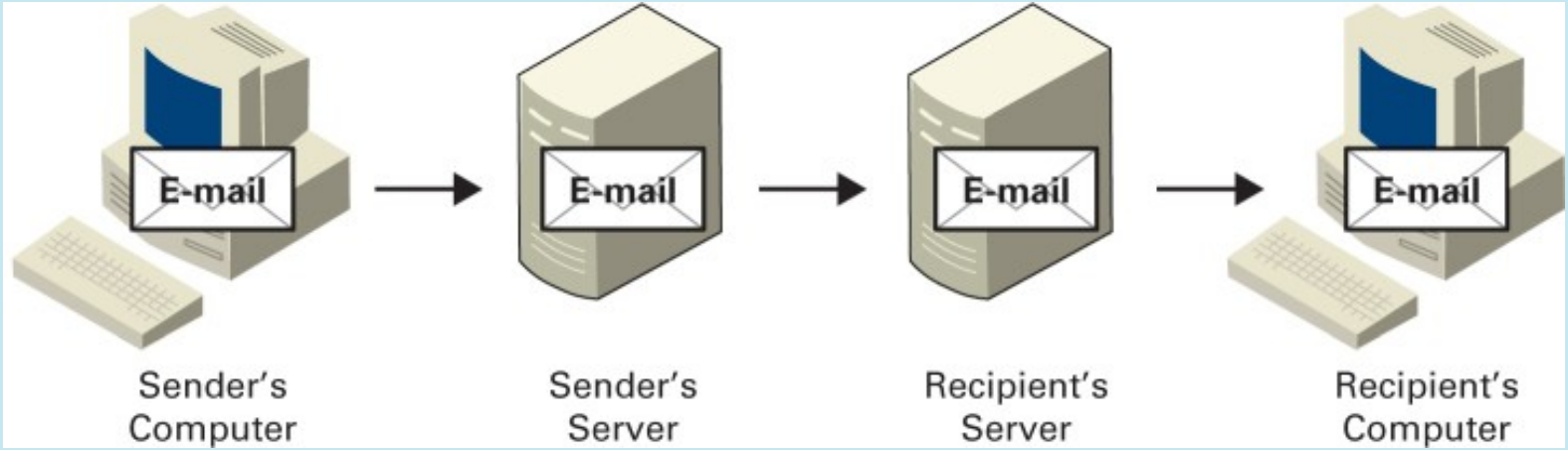
# PRIVACY

- ***Privacy*** – the right to left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent
- Dimensions of privacy
  - Psychological: to have a sense of control
  - Legal: to be able to protect yourself

# Privacy and Other Individuals

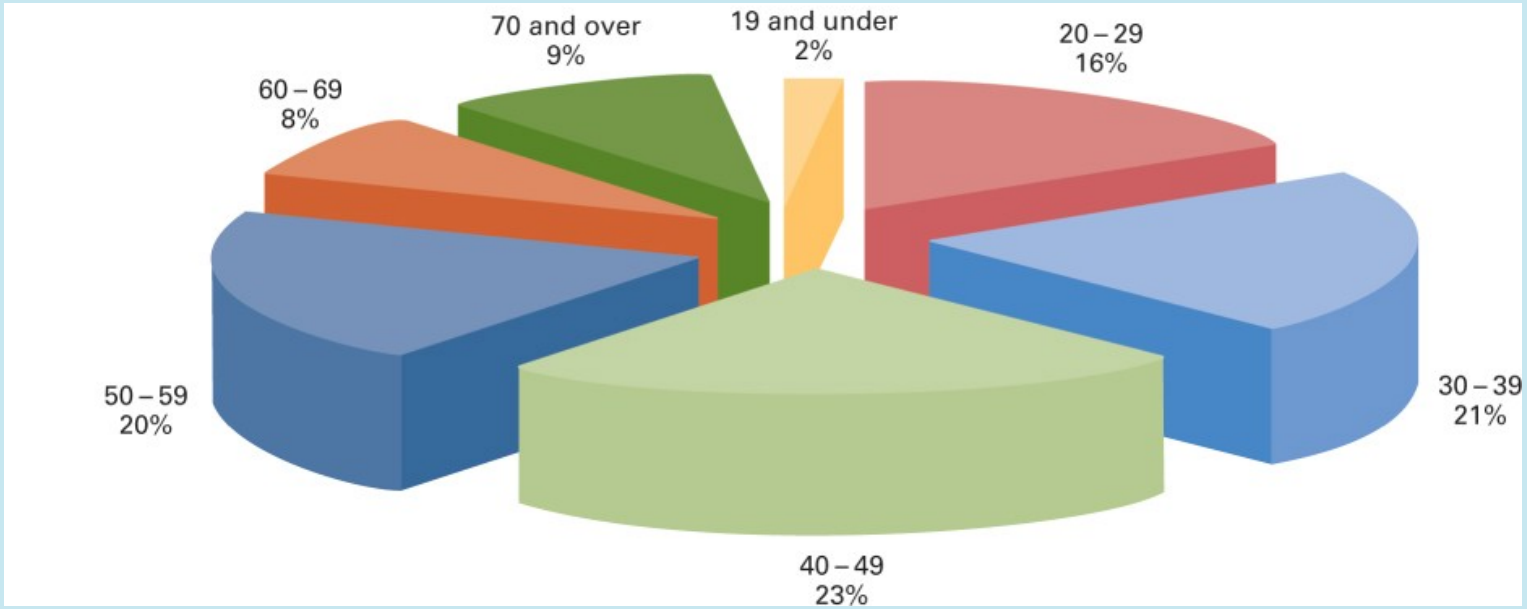
- ***Key logger (key trapper) software*** – a program that, when installed on a computer, records every keystroke and mouse click
- Screen capture programs – capture screen from video card
- E-mail is stored on many computers as it travels from sender to recipient
- ***Hardware key logger*** – hardware device that captures keystrokes moving between keyboard and motherboard.
- Event Data Recorders (EDR) – located in the airbag control module and collects data from your car as you are driving.

# An E-Mail is Stored on Many Computers



# Identity Theft

- ***Identity theft*** – the forging of someone's identity for the purpose of fraud



# Identity Theft

- ***Phishing (carding, brand spoofing)*** – a technique to gain personal information for the purpose of identity theft
- NEVER
  - Reply without question to an e-mail asking for personal information
  - Click directly on a Web site provided in such an e-mail

# Identity Theft

**Some Facts on Phishing . . .**

- In January 2004 there were 198 phishing sites, but by February 2005 that number had risen to 2,625, according to the Anti-Phishing Working Group.
- The same group says that the number of unique phishing e-mails reached 13,141 in February of 2004.
- Symantec says that its Brightmail spam filters blocked an average of 33 million phishing attempts per week in December 2004, compared to an average of only 9 million during the previous July.
- The Phemon Institute says consumers lost $500 million to phishers in 2004.
- Also from the Phemon Institute: Of 1,335 people surveyed, about 70 percent visited a fake site, and as many as 15 percent said they had provided personal information to the fake site.

**. . . And What to Do If You Suspect You're at Risk**

The FTC says that if you believe your personal information may have been compromised, you should:

- Close your credit-card accounts (using an ID Theft Affidavit form) and change all your passwords.
- Place a fraud alert on your credit reports with one of the major credit bureaus (Equifax, Experian, and TransUnion).
- Ask government agencies like the Department of Motor Vehicles to flag your file so that no one can get documents in your name.

# Pharming

- ***Pharming*** - rerouting your request for a legitimate Web site
  - sending it to a slightly different Web address
  - or by redirecting you after you are already on the legitimate site
- Pharming is accomplished by gaining access to the giant databases that Internet providers use to route Web traffic.
- It often works because it's hard to spot the tiny difference in the Web site address.

# Privacy and Employees

- Companies need information about their employees to run their business effectively
- As of March 2005, 60% of employers monitored employee e-mails
- 70% of Web traffic occurs during work hours
- 78% of employers reported abuse
- 60% employees admitted abuse

# Privacy and Employees

- Cyberslacking – misuse of company resources
- Visiting inappropriate sites
- Gaming, chatting, stock trading, social networking, etc.

# Reasons for Monitoring

- Hire the best people possible
- Ensure appropriate behavior on the job
- Avoid litigation for employee misconduct

# Privacy and Consumers

- Consumers want businesses to
  - Know who they are, but not to know too much
  - Provide what they want, but not gather information on them
- Let them know about products, but not pester them with advertising

# Cookies

- ***Cookie*** – a small file that contains information about you and your Web activities, which a Web site places on your computer
- Handle cookies by using
  - Web browser cookie management option
  - Buy a program that manages cookies

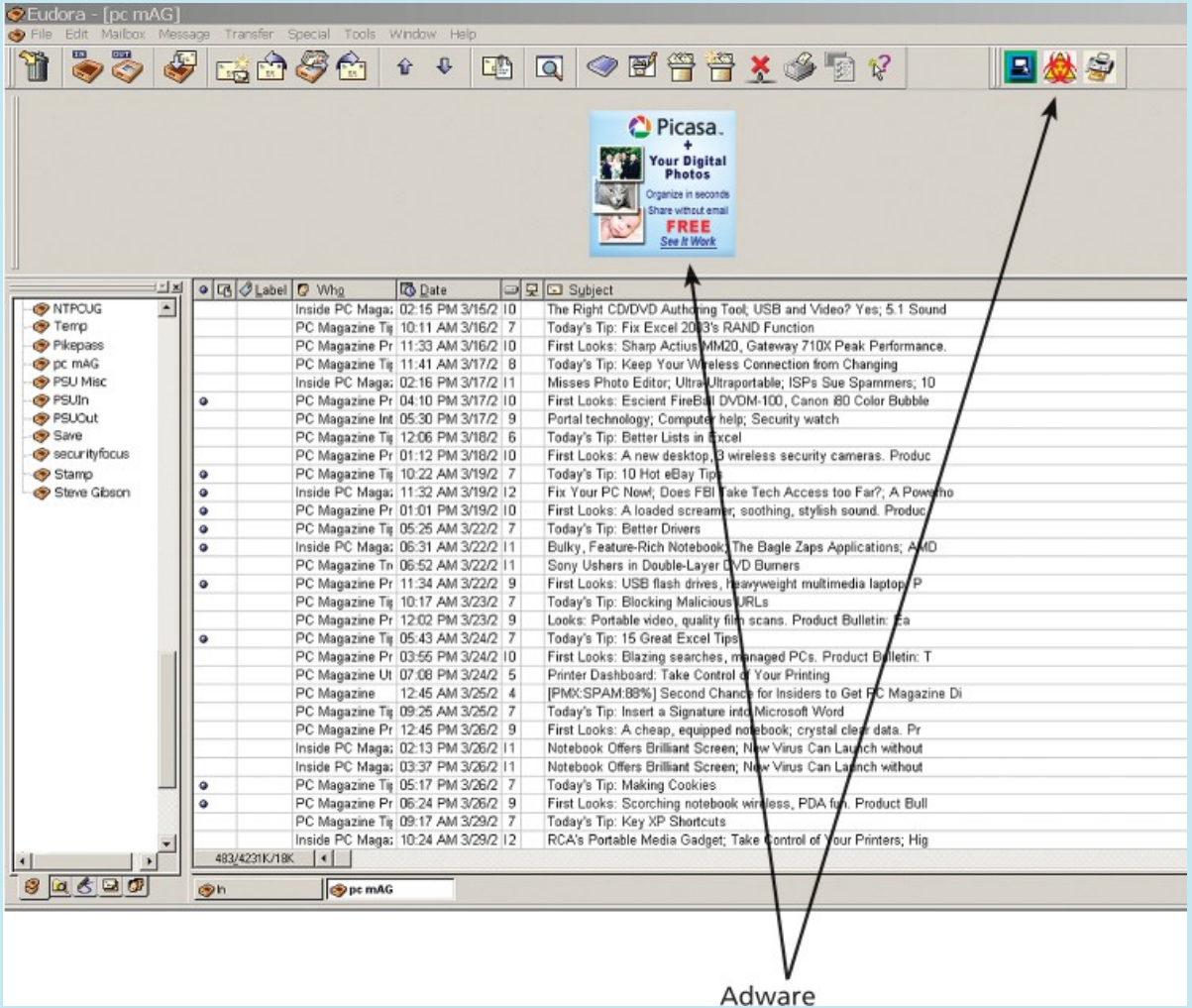
# Spam

- ***Spam*** – unsolicited e-mail from businesses advertising goods and services
- Gets past spam filters by
  - Inserting extra characters
  - Inserting HTML tags that do nothing
  - Replying usually increases, rather than decreases, amount of spam

# Adware and Spyware

- ***Adware*** – software to generate ads that installs itself when you download another program
- ***Spyware (sneakware, stealthware)*** – software that comes hidden in downloaded software and helps itself to your computer resources

# Adware in Free Version of Eudora



# Trojan Horse Software

- ***Trojan horse software*** – software you don't want inside software you do want
- Some ways to detect Trojan horse software
  - AdAware at www.lavasoftUSA.com
  - The Cleaner at www.moosoft.com
  - Trojan First Aid Kit (TFAK) at www.wilders.org
  - Check it out before you download at www.spychecker.com

# Web Logs

- ***Web log*** – one line of information for every visitor to a Web site
- ***Clickstream*** – records information about you during a Web surfing session such as what Web sites you visited, how long you were there, what ads you looked at, and what you bought.
- ***Anonymous Web browsing (AWB***) – hides your identity from the Web sites you visit
  - The Anonymizer at www.anonymizer.com
  - SuftSecret at www.surfsecret.com

# Privacy and Government Agencies

- About 2,000 government agencies have databases with information on people
- Government agencies need information to operate effectively
- Whenever you are in contact with government agency, you leave behind information about yourself

# Government Agencies Storing Personal Information

- Law enforcement
  - NCIC (National Crime Information Center)
  - FBI
- Electronic Surveillance
  - Carnivore or DCS-1000
  - Magic Lantern (software key logger)
  - NSA (National Security Agency)
  - Echelon collect electronic information by satellite

# Government Agencies Storing Personal Information

- IRS
- Census Bureau
- Student loan services
- FICA
- Social Security Administration
- Social service agencies
- Department of Motor Vehicles

# Laws on Privacy

- *Health Insurance Portability and Accountability Act (HIPAA)* protects personal health information
- *Financial Services Modernization Act* requires that financial institutions protect personal customer information
- Other laws in Figure 8.6 on page 356

# SECURITY AND EMPLOYEES

- Attacks on information and computer resources come from inside and outside the company
- Computer sabotage costs about $10 billion per year
- In general, employee misconduct is more costly than assaults from outside

# Security and Employees

| | Who's Committing Fraud |
|---|---|
| 61% | Fraud committed by men |
| 39% | Fraud committed by women |
| $250,000 | Median loss from fraud committed by men |
| $102,000 | Median loss from fraud committed by women |
| 41% | Fraud committed by managers |
| 39.5% | Fraud committed by employees |
| 19.3% | Fraud committed by owners/executives |

# Security and Outside Threats

- ***Hackers*** – knowledgeable computer users who use their knowledge to invade other people's computers
- ***Computer virus (virus)*** – software that is written with malicious intent to cause annoyance or damage
- ***Worm*** – type of virus that spreads itself from computer to computer usually via e-mail
- ***Denial-of-service (DoS) attack*** – floods a Web site with so many requests for service that it slows down or crashes

# Computer Viruses Can't

- Hurt your hardware
  - Ex: Monitors, printers, processors, etc.
- Hurt any files they weren't designed to attack
  - Ex: A worm designed to attack Outlook won't attack other e-mail programs
- Infect files on write-protected media

# Security Measures

- ***Anti-virus software*** – detects and removes or quarantines computer viruses
- *Anti*-spyware and anti-adware software
- Spam protection software – identifies and marks and/or deletes Spam
- Anti-phishing software **–** lets you know when phishing attempts are being made
- ***Firewall*** – hardware and/or software that protects a computer or network from intruders

# Security Measures

- Anti-rootkit software – stops outsiders taking control of your machine
- ***Encryption*** – scrambles the contents of a file so that you can't read it without the decryption key
- ***Public Key Encryption (PKE)*** – an encryption system with two keys: a public for everyone and a private one for the recipient
- ***Biometrics*** – the use of physiological characteristics for identification purposes