Computer Security and Safety, Ethics, and Privacy

Discovering Computers & Microsoft Office 2007
A Fundamental Combined Approach
Objectives Overview

Describe various types of network attacks, and identify ways to safeguard against these attacks, including firewalls and intrusion detection software.

Discuss techniques to prevent unauthorized computer access and use.

Identify safeguards against hardware theft and vandalism.

Explain the ways to protect against software theft and information theft.

See Page 181 for Detailed Objectives
Objectives Overview

- Discuss the types of devices available that protect computers from system failure
- Identify risks and safeguards associated with wireless communications
- Discuss ways to prevent health-related disorders and injuries due to computer use
- Discuss issues surrounding information privacy

See Page 181 for Detailed Objectives

Discovering Computers and Microsoft Office 2007
Chapter 5
A computer security risk is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability.

A cybercrime is an online or Internet-based illegal act.
Computer Security Risks

- Internet and network attacks
  - VIRUS ATTACK
- unauthorized access and use
  - INTERCEPTING WIRELESS COMMUNICATIONS
- hardware theft
  - STOLEN COMPUTER
- system failure
  - LIGHTNING STRIKE
- information theft
  - STOLEN IDENTITY
- software theft
  - ILLEGAL COPYING

Secure Computer Environment

Discovering Computers and Microsoft Office 2007
Chapter 5
Internet and Network Attacks

• Information transmitted over networks has a higher degree of security risk than information kept on an organization’s premises

**Computer Virus**
• Affects a computer negatively by altering the way the computer works

**Worm**
• Copies itself repeatedly, using up resources and possibly shutting down the computer or network

**Trojan Horse**
• A malicious program that hides within or looks like a legitimate program

**Rootkit**
• Program that hides in a computer and allows someone from a remote location to take full control
Video: Attack of the Mobile Viruses

CLICK TO START

Discovering Computers and Microsoft Office 2007
Chapter 5
Internet and Network Attacks

• An infected computer has one or more of the following symptoms:

  - Operating system runs much slower than usual
  - Available memory is less than expected
  - Files become corrupted
  - Screen displays unusual message or image
  - Music or unusual sound plays randomly
  - Existing programs and files disappear
  - Programs or files do not work properly
  - Unknown programs or files mysteriously appear
  - System properties change
  - Operating system does not start up
  - Operating system shuts down unexpectedly
Internet and Network Attacks

How a Virus Can Spread through an E-Mail Message

Step 1
Unscrupulous programmers create a virus program that deletes all files. They hide the virus in a word processing document and attach the document to an e-mail message.

Step 2
They send the e-mail message to thousands of users around the world.

Step 3a
Some users open the attachment and their computers become infected with the virus.

Step 3b
Other users do not recognize the name of the sender of the e-mail message. These users do not open the e-mail message — instead they immediately delete the e-mail message and continue using their computers. These users’ computers are not infected with the virus.
Internet and Network Attacks

- Users can take several precautions to protect their home and work computers and mobile devices from these malicious infections

Tips for Preventing Viruses and Other Malware

1. Never start a computer with removable media inserted in the drives or plugged in the ports, unless the media are uninfected.
2. Never open an e-mail attachment unless you are expecting it and it is from a trusted source.
3. Set the macro security in programs so that you can enable or disable macros. Enable macros only if the document is from a trusted source and you are expecting it.
4. Install an antivirus program on all of your computers. Update the software and the virus signature files regularly.
5. Scan all downloaded programs for viruses and other malware.
6. If the antivirus program flags an e-mail attachment as infected, delete or quarantine the attachment immediately.
7. Before using any removable media, scan the media for malware. Follow this procedure even for shrink-wrapped software from major developers. Some commercial software has been infected and distributed to unsuspecting users.
8. Install a personal firewall program.
9. Stay informed about new virus alerts and virus hoaxes.
Internet and Network Attacks
Internet and Network Attacks

- A **botnet** is a group of compromised computers connected to a network
  - A compromised computer is known as a **zombie**
- A **denial of service attack (DoS attack)** disrupts computer access to Internet services
- A **back door** is a program or set of instructions in a program that allow users to bypass security controls
- **Spoofing** is a technique intruders use to make their network or Internet transmission appear legitimate
Internet and Network Attacks

• **A firewall** is hardware and/or software that protects a network’s resources from intrusion.
Internet and Network Attacks

Intrusion detection software

• Analyzes all network traffic
• Assesses system vulnerabilities
• Identifies any unauthorized intrusions
• Notifies network administrators of suspicious behavior patterns or security breaches
Unauthorized access is the use of a computer or network without permission.

Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities.
Unauthorized Access and Use

Access controls define who can access a computer, when they can access it, and what actions they can take

- Two-phase processes called identification and authentication
- User name
- Password
- CAPTCHA
Unauthorized Access and Use

- A **possessed object** is any item that you must carry to gain access to a computer or computer facility
  - Often are used in combination with a **personal identification number (PIN)**

- A **biometric device** authenticates a person’s identity by translating a personal characteristic into a digital code that is compared with a digital code in a computer
Unauthorized Access and Use

• **Digital forensics** is the discovery, collection, and analysis of evidence found on computers and networks

• Many areas use digital forensics

- Law enforcement
- Criminal prosecutors
- Military intelligence
- Insurance agencies
- Information security departments
Hardware Theft and Vandalism

**Hardware Theft** is the act of stealing computer equipment.

**Hardware Vandalism** is the act of defacing or destroying computer equipment.
Hardware Theft and Vandalism

- To help reduce the chances of theft, companies and schools use a variety of security measures.

<table>
<thead>
<tr>
<th>Security Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical access controls</td>
</tr>
<tr>
<td>Alarm systems</td>
</tr>
<tr>
<td>Cables to lock equipment</td>
</tr>
<tr>
<td>Real time location system</td>
</tr>
<tr>
<td>Passwords, possessed objects, and biometrics</td>
</tr>
</tbody>
</table>

Click to view Web Link, click Chapter 5, Click Web Link from left navigation, then click RTLS below Chapter 5.
Software Theft

• **Software theft** occurs when someone:

- Steals software media
- Intentionally erases programs
- Illegally copies a program
- Illegally registers and/or activates a program
Software Theft

A single-user **license agreement** typically contains the following conditions:

**Permitted to**
- Install the software on one computer
- Make one copy of the software
- Remove the software from your computer before giving it away or selling it

**Not permitted to**
- Install the software on a network
- Give copies to friends or colleagues while continuing to use the software
- Export the software
- Rent or lease the software
Software Theft

• Copying, loaning, borrowing, renting, or distributing software can be a violation of copyright law

• Some software requires product activation to function fully
Information Theft

• **Information theft** occurs when someone steals personal or confidential information

• **Encryption** is a process of converting readable data into unreadable characters to prevent unauthorized access

<table>
<thead>
<tr>
<th>Simple Encryption Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Transposition</td>
</tr>
<tr>
<td>Substitution</td>
</tr>
<tr>
<td>Expansion</td>
</tr>
<tr>
<td>Compaction</td>
</tr>
</tbody>
</table>
Information Theft

• A **digital signature** is an encrypted code that a person, Web site, or organization attaches to an electronic message to verify the identity of the sender

• A **digital certificate** is a notice that guarantees a user or a Web site is legitimate
  
  – Issued by a **certificate authority**
Information Theft

indicates secure Web page
System Failure

• A system failure is the prolonged malfunction of a computer

• A variety of factors can lead to system failure, including:
  – Aging hardware
  – Natural disasters
  – Electrical power problems
  – Errors in computer programs
System Failure

- Two ways to protect from system failures caused by electrical power variations include surge protectors and uninterruptable power supplies (UPS).
Backing Up – The Ultimate Safeguard

• A **backup** is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed
  – To **back up** a file means to make a copy of it

• Offsite backups are stored in a location separate from the computer site
Backing Up – The Ultimate Safeguard

- Two categories of backups:
  - Full backup
  - Selective backup

- Three-generation backup policy

  Grandparent
  ↓
  Parent
  ↓
  Child
Wireless Security

• Wireless access poses additional security risks
  – About 80 percent of wireless networks have no security protection

• War driving allows individuals to detect wireless networks while driving a vehicle through the area

A wireless access point should not broadcast a network name
Change the default network name
Configure a WAP so that only certain devices can access it
Use WPA or WPA2 security standards
Health Concerns of Computer Use

• The widespread use of computers has led to health concerns
  – **Repetitive strain injury** (RSI)
    • Tendonitis
    • Carpal tunnel syndrome (CTS)
  – **Computer vision syndrome** (CVS)

**Hand Exercises**

• Spread fingers apart for several seconds while keeping wrists straight.
• Gently push back fingers and then thumb.
• Dangle arms loosely at sides and then shake arms and hands.
Health Concerns of Computer Use

Techniques to Ease Eyestrain

- Every 10 to 15 minutes, take an eye break.
  - Look into the distance and focus on an object for 20 to 30 seconds.
  - Roll your eyes in a complete circle.
  - Close your eyes and rest them for at least one minute.
- Blink your eyes every five seconds.
- Place your display device about an arm’s length away from your eyes with the top of the screen at eye level or below.
- Use large fonts.
- If you wear glasses, ask your doctor about computer glasses.
- Adjust the lighting.
Health Concerns of Computer Use

- Ergonomics is an applied science devoted to incorporating comfort, efficiency, and safety into the design of items in the workplace.
Health Concerns of Computer Use

- **Computer addiction** occurs when the computer consumes someone’s entire social life.

- Symptoms of users include:
  - Craves computer time
  - Overjoy when at the computer
  - Unable to stop computer activity
  - Irritable when not at the computer
  - Neglects family and friends
  - Problems at work or school
Ethics and Society

- **Computer ethics** are the moral guidelines that govern the use of computers and information systems
- Information accuracy is a concern
  - Not all information on the Web is correct
Ethics and Society

Intellectual property rights are the rights to which creators are entitled for their work

- A **copyright** protects any tangible form of expression

Digital rights management is a strategy designed to prevent illegal distribution of movies, music, and other digital content
Ethics and Society

- **Green computing** involves reducing the electricity and environmental waste while using a computer.

  **ENERGY STAR program**

---

**Green Computing Suggestions**

1. Use computers and devices that comply with the ENERGY STAR program.
2. Do not leave the computer running overnight.
3. Turn off the monitor, printer, and other devices when not in use.
4. Use LCD monitors instead of CRT monitors.
5. Use paperless methods to communicate.
6. Recycle paper.
7. Buy recycled paper.
8. Recycle toner cartridges.
9. Recycle old computers, printers, and other devices.
10. Telecommute (saves gas).
11. Use video conferencing and VoIP for meetings.
Ethics and Society

- **Information privacy** refers to the right of individuals and companies to deny or restrict the collection and use of information about them.
- Huge databases store data online.
- It is important to safeguard your information.
### How to Safeguard Personal Information

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

- When you fill out a form, the merchant that receives the form usually enters it into a database.
- Many companies today allow people to specify whether they want their personal information distributed.
Ethics and Society

- A **cookie** is a small text file that a Web server stores on your computer.
- Web sites use cookies for a variety of reasons:
  - Allow for personalization
  - Store users’ passwords
  - Assist with online shopping
  - Track how often users visit a site
  - Target advertisements

Click to view Web Link, click Chapter 5, Click Web Link from left navigation, then click Cookies below Chapter 5
How Cookies Work

**Step 1**
When you type the Web address of a Web site in a browser window, the browser program searches your hard disk for a cookie associated with the Web site.

**Step 2**
If the browser finds a cookie, it sends information in the cookie file to the Web site.

**Step 3**
If the Web site does not receive cookie information, and is expecting it, the site creates an identification number for you in its database and sends that number to your browser. The browser in turn creates a cookie file based on that number and stores the cookie file on your hard disk. The Web site now can update information in the cookie file whenever you access the site.
Ethics and Society

- **Spam** is an unsolicited e-mail message or newsgroup posting.
- **E-mail filtering** blocks e-mail messages from designated sources.
- **Anti-spam programs** attempt to remove spam before it reaches your inbox.
Ethics and Society

- **Phishing** is a scam in which a perpetrator sends an official looking e-mail message that attempts to obtain your personal and financial information.

- **Pharming** is a scam where a perpetrator attempts to obtain your personal and financial information via spoofing.
Ethics and Society

• The concern about privacy has led to the enactment of federal and state laws regarding the storage and disclosure of personal data
  – See Figure 10-25 on page 406 for a listing of major U.S. government laws concerning privacy
Social engineering is defined as gaining unauthorized access or obtaining confidential information by taking advantage of trust and naivety.

Employee monitoring involves the use of computers to observe, record, and review an employee’s use of a computer.
Ethics and Society

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

Potential computer risks and the safeguards

Wireless security risks and safeguards

Computer-related health issues and preventions

Ethical issues surrounding information accuracy, intellectual property rights, green computing, and information privacy
Chapter Five

Computer Security and Safety, Ethics, and Privacy

Discovering Computers & Microsoft Office 2007
A Fundamental Combined Approach

Chapter 5 Complete