Lesson 31
Computer Safety and Ethics

Computer Literacy BASICS: A Comprehensive Guide to IC^3, 4th Edition

Objectives

- Maintain a safe computing environment.
- Prevent computer-related injuries.
- Identify security risks.
- Set access restrictions.
- Understand workplace privacy.
- Avoid e-commerce problems.

Objectives (continued)

- Protect privacy on the Internet.
- Use the Internet safely and legally.
- Practice responsibility as a computer user.

Vocabulary

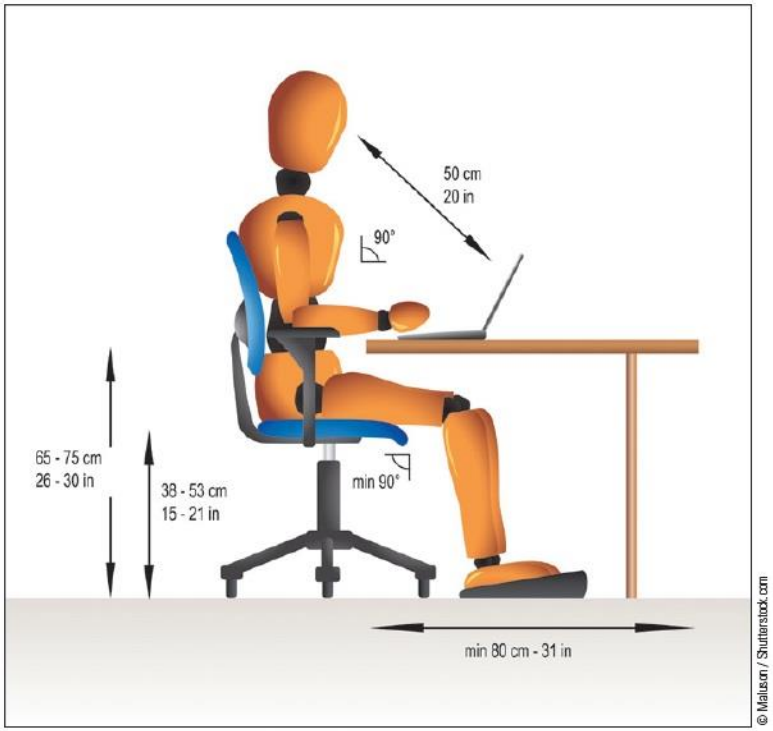
- browser hijacking
- brute force attacks
- hacking
- hardware firewall
- keylogger
- private key
- public key
- repetitive strain injury (RSI)
- sniffer
- spyware
- strong password
- Transport Layer Security (TLS)

Maintaining a Safe Computing Environment

- Make sure you use a computer in a way that supports your comfort, health, and safety.
- Pay attention to your posture, lighting, and activity level.
- Review product safety guidelines provided with your computer or any other electronic device.
- See *www.osha.gov* for guidelines.

Preventing Computer-Related Injuries

- Take precautions to avoid chronic physical maladies such as eyestrain, back problems, and repetitive strain injury (RSI), which can result when a person makes too many of the same motions over a long period of time.



Identifying Security Risks

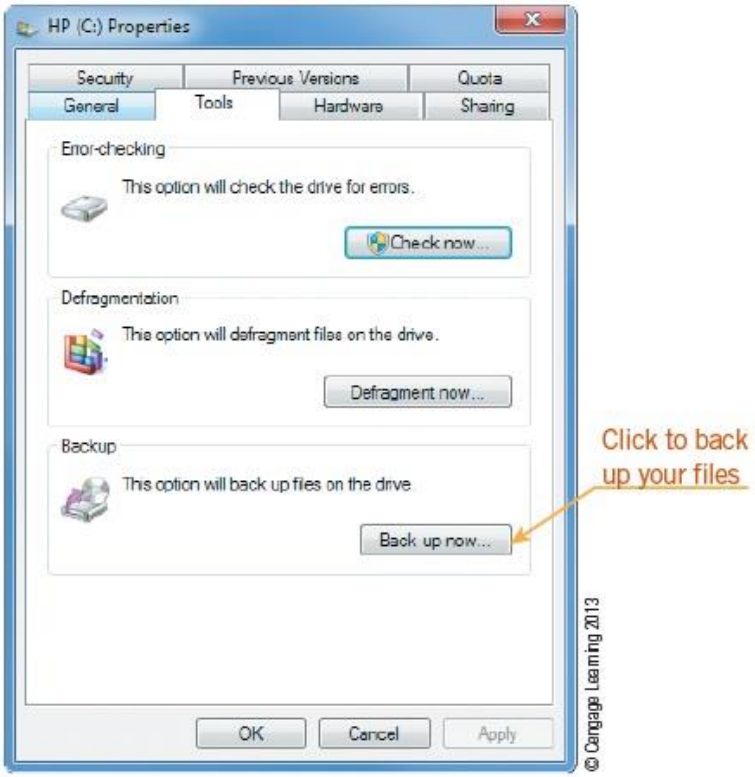
- An intruder could use a sniffer, which is a program that hackers use to capture user names and passwords on a network.
- **Using Network Protection:**
- When setting up a wireless network, change the default password and turn on some form of encryption.

Identifying Security Risks (continued)

- **Computer Hacking:**
- Computer hacking involves invading someone else's computer, usually for personal gain or the satisfaction of defeating a security system.
- If the network is large, a hardware firewall that controls the computers from one point should be implemented.

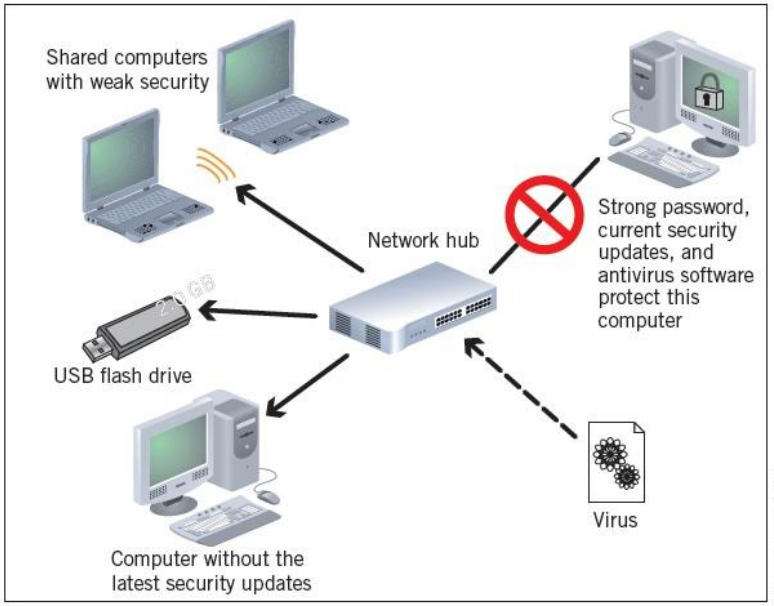
Identifying Security Risks (continued)

- **Avoiding Data Loss:**
- Save frequently.
- Use surge protectors.
- Back up important files regularly.



Identifying Security Risks (continued)

- **Safeguarding Data Against Software Threats:**
- Use strong passwords, install latest security updates, use an up-to-date antivirus program.

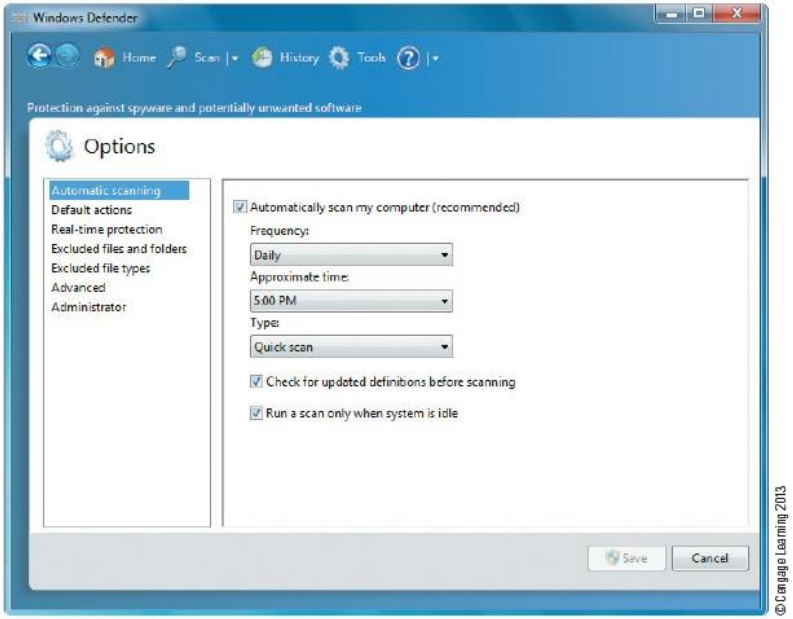


Identifying Security Risks (continued)

- **Safeguarding Data Against Software Threats (continued):**
- A strong password is both complex and secure.
- Strong passwords are more resistant to brute force attacks, which use a script or program to log on to an account using hundreds of words or phrases stored in a dictionary file.
- A keylogger is a malicious program that records keystrokes.

Identifying Security Risks (continued)

- **Safeguarding Data Against Software Threats (continued):**
- Hackers often use spyware to control your browser, a practice called browser hijacking.
- You can also use antispyware software such as Windows Defender to protect your system.



Setting Access Restrictions

- System administrators and users often restrict access to files, storage devices, computers, networks, the Internet, or specific Internet sites to protect data and other users.
- Software is available that lets you monitor computer usage, including Web sites, e-mail messages, social networks, instant messaging and chats, and applications.

Understanding Workplace Privacy

- Any information gathered from a company's computer system is company property and not an individual worker's personal property. The employee normally has no right to personal privacy regarding those issues.
- Many organizations have computer or network usage policies that provide guidelines for using the organization's systems ethically, professionally, and legally.

Avoiding E-Commerce Problems

- Before providing personal information or credit card information on an e-commerce or similar site, first verify that the site is secure.

Avoiding E-Commerce Problems (continued)

- Several companies provide a Transport Layer Security (TLS) or Secure Sockets Layer (SSL) certificate for e-commerce sites, sites that process sensitive data, and sites that require privacy and security requirements.
- An SSL certificate consists of a public key and a private key. The public key encrypts information and the private key deciphers the information.

Protecting Privacy on the Internet

- Phishing is a type of computer fraud that attempts to steal your private data.

Protecting Privacy on the Internet (continued)

- **Cookies and Spyware:**
- Clean up the unnecessary cookies on your computer frequently with a utility program designed for that purpose.
- Spyware can be harmful as well as annoying.
- **Securing Data:**
- The best way to protect data is to effectively control the access to it.
- Use strong passwords, use code names or aliases, and always sign off of public computers.

Using the Internet Safely and Legally

- Nearly all institutions have written policies and guidelines regarding Internet usage.
- The Department of Justice and other government agencies provide resources for Internet safety.

Practicing Responsibility as a Computer User

- It is your responsibility to stay informed about changes and advancements in computer technology, product upgrades, and virus threats.
- Recycle products such as used computer paper and ink cartridges.

Summary

In this lesson, you learned:

- Make sure you use a computer in a way that supports your comfort, health, and safety. When you use a computer, take precautions to avoid chronic physical maladies such as repetitive motion injuries, eyestrain, and back problems that can arise over time. Ergonomic design, which adapts equipment and the workplace to fit the worker, can help to prevent repetitive strain injuries.

Summary (continued)

- When setting up your wireless network, your first step should be to change the default password to protect access to the network.
- Computer hacking involves invading someone else's computer, usually for personal gain or the satisfaction of defeating a security system.
- To avoid data loss, you can use techniques and devices for preventing power interruptions. You can also devise and follow a regular procedure for backing up your data.

Summary (continued)

- A virus is a program that has been written, usually by a hacker, to corrupt data on a computer. The virus is attached to a file and spreads from one file to another when the program is executed. To protect your computer against virus damage, use up-to-date antivirus software, download and install security updates for your operating system, and avoid opening files sent via e-mail from people you do not know.

Summary (continued)

- System administrators and users often restrict access to files, storage devices, various computers, networks, the Internet, or specific Internet sites.
- If you work for a company that provides you with e-mail services, the information you send is available to the company and is the company's property.

Summary (continued)

- TSL and SSL technology enables encryption of sensitive information by establishing a private communication channel. Data transmitted through this channel is encrypted during transmission.
- Nearly all schools, government agencies, companies, libraries, and other similar institutions have written policies and guidelines regarding Internet usage.