Chapter 16 - Security, Privacy, and Safety
16.1 - Preventing Computer Threats Section

Grading:
Notes: _____/20
Lesson Review: _____/20
Research Cookies: _____/20
Record Cookies: _____/20
Beware Spyware: _____/20
Total points: _____/100

Essential Question

- What impact do computer threats have on our economy?

Section 16.1 Learning Goals

After completing this section, you will be able to:

- Identify types of computer threats.
- Discuss Internet security protocols.
- Explain how to protect stored data.

Competencies

- 6670.57 Describe the importance of system maintenance and preventive measures, including the consequences of not taking preventive measures.
- 6670.64 Identify basic security risks inherent to computer hardware and software.
- 6670.65 Describe security best practices for businesses.
- 66970.66 Describe the importance of data backup media and strategies

Terms

- adware
- antivirus software
- bot
- cache
- censorship
- completely automated public Turing test to tell computers and humans apart (CAPTCHA)
- computer virus
- computer worm
- cookies
- horse
- data vandalism
- hacking
- malware
- phishing
- pop-up
- ransomware
- scareware
- social engineering
- spyware
- Trojan

Computer Threats

- **Malware** is software that intentionally performs actions to _____ the operation of a computer system, collect private information, or otherwise harm the

computer or user

- Malicious software
- Broad category of _____ software
- **Computer viruses** consist of computer code carried in another program that can _____ itself in order to corrupt or otherwise harm either data files or the software used to process these files
- **Computer worm** is similar to a virus, but can _____ to other computers
- **Trojan horse** is a program that invited the user to run it while _____ malicious code that will be executed
- **Spyware** is software that _____ collects a user's data and behavior
- **Adware** is software that creates advertisements designed to _____ the user to another website

Activity	Action and Reason
Pop-up dialog boxes	Do not click links within pop-up dialog boxes. Just clicking within the dialog box or a "close" button within the window may result in spyware being installed. Instead, close the pop-up dialog box by clicking on the standard close button (X) in the upper-right corner of the title bar.
Pop-up windows on websites	These are windows created using HTML or other website-formatting language. They can be recognized because they do not look like standard dialog boxes generated by the operating system. Often, all parts of a pop-up window, including what appears to be a standard close button (X), will activate spyware. Try pressing the [Esc] key to close the window or close the browser window.
Unexpected dialog boxes	Be suspicious of unexpected dialog boxes that ask whether you want to run a particular program or perform another type of task. Close the dialog box by clicking the standard close button (X) in the title bar.
Links offering antispyware software	These links may actually install the spyware it claims to be eliminating. Only install antispyware from the developer's website, not from a third-party site.

Goodheart-Willcox Publisher

- **Scareware** is software designed to cause enough _____ so the computer user leaps at the chance to opt for a poor choice
- **Ransomware** encrypts files or _____ the user's access to programs until the user pays to unlock them
- **Social engineering** involves manipulative techniques designed to lure unwary computer users into launching an _____ file or opening a link to an infected website
    - Invitation to open an _____ love letter or a notice of a traffic ticket
    - E-mail that _____ technical messages issued by the user's e-mail
    - Message that claims to have been _____ from Microsoft
    - Offer to _____ scandalous information on a famous person
    - Bank notice asking the customer to _____ account numbers or access codes
    - Attractively _____ files that entice the user to download them
    - PasswordHacker.exe
    - MicrosoftCDKeyGenerator.exe

    - JobsPayingMillions.exe
    - PlayStationEmulator.exe
    - FreeInternetAccess.exe
- **Cookies** are small text files that _____ put on the computer hard disk drive
- **Cache** is location of files _____ stored on computer's hard drive
    - Files from Internet, such as website graphics
    - Cookies
    - Clear cache to remove these files
- **Pop-up** is a window that appears on top of or under the _____ web page
    - Considered spam
    - May contain malware
- **Phishing** is an attempt to get _____ information by appearing as a harmless request
- **Data vandalism** is the manipulation or _____ of data found in cyberspace
- Computer Hacking
    - **Hacking** is an activity by computer programmers to _____ into the e-mails, websites, computer systems, and files of other computer users
    - Often _____ and illegal, but may be legitimate
    - Numerous ways to hack a computer
- **Censorship** is the act of _____ access to information or removing information to prevent the information from being seen
    - Must balance between safe computing environment and free access
    - Justified in many cases
        - Prevent _____ of computers and time
        - Protect reputation of organization
    - Internet Security Protocols
- TCP/IP
    - Sniffing
    - Denial of service attacks
- SSH
    - _____ shell secures data communication
    - TLP, UAP, CP
- HTTPS
    - _____ communication over computer networks
    - Authenticates website to web server
- Other Protocols
    - FTP, SMTP
    - Bitcoin
- Security Measures
    - **Bot** is a software application that automatically _____ Internet-based activities
    - **Completely automated public Turing test to tell computers and humans apart**

(CAPTCHA) is a brief online test to determine whether the _____ for access comes from a computer or a human
    - Protecting Stored Data
- Removing _____ from Discarded Devices
    - Storage devices
        - Wipes
        - Mechanically destroyed
- Defending Against Cyber Attacks
    - **Antivirus software** is cyber-defense software that detects and _____ malicious software from a computer
    - Must be regularly updated

Section 16.1 Review

1. What type of malware encrypts files or blocks access to programs until a user pays to unlock them?
    a. Shareware
    b. Ransomware
    c. Scareware
    d. Adware
2. What network protocol secures data communication and remote command execution?
    a. TCP/IP
    b. POP
    c. SSH
    d. WAN
3. What is the name of a program that invites the user to run it while concealing malicious code that will be executed?
    a. Computer virus
    b. Computer worm
    c. Trojan horse
    d. Spyware
4. Current antivirus software protects against _____.
    a. All possible threats
    b. All known threats
    c. Most known threats
    d. No known threats
5. What is the cache?
    a. A location on the computer's hard drive where temporary files are stored
    b. The purchase price of a computer system, including all peripherals
    c. A set amount of a video file that is downloaded before it begins to play

6. Which of the following is a measure to assure data is entered by a human?
    a. Hackers
    b. Corrupted files
    c. Malware
    d. CAPTCHA
7. _____ T/F Hacking is legitimate when a company hires a hacker to find flaws in the security system.
8. _____ T/F Internet protocols tell computers, modems, routers, and networks how to communicate with each other.
9. _____ T/F Antivirus software protects against any physical threat to the computer
10. _____ T/F Scareware is software designed to cause enough anxiety so the computer user leaps at the chance to opt for a poor choice.

Research Cookies

In this project you will research cookies (on your computer) and then create a PowerPoint presentation based on this topic. Additionally, include at least one related graphic on each slide.

Slide 1: Define Web cookies.

Slide 2: What's good about cookies?

Slide 3: What's bad about cookies?

Slide 4: How can you get rid of cookies?

Slide 5: How are cookies used for Internet shopping?

You will be recording your presentation, prior to submitting it.

Beware of Spyware

As described in this lesson, the Internet makes widespread publication of information easy. The ease of obtaining information from the Internet and of publishing information on the Internet can contribute to legal problems.

1. Access the FTC Web site at https://www.consumer.ftc.gov/media/game-0002-beware-spyware
2. Play the Beware of Spyware game on this site and click any related links.
3. Prepare a report on what you learned. Include information on how to avoid spyware. Minimum 2 paragraphs.