Component 4: Introduction to Information and Computer Science

Unit 2: Internet and the World Wide Web

Unit Objectives

- Definition of the Internet and World Wide Web.
- Connecting to the Internet.
- Searching the Internet, filtering results and evaluating credibility of results.
- Internet security and privacy concerns.
- Ethical considerations of the Internet.
- Online healthcare applications and associated security and privacy issues (including HIPAA).

What Devices are Usually Attacked?

- Routers
  - ✓ Sends traffic from a private network to the Internet and from the Internet to a private network.
  - ✓ If a hacker can successfully attack a router:
    - All network traffic can be viewed.
    - Traffic can be redirected to the hacker's equipment.

What Devices are Usually Attacked? (cont'd)

- Web Servers
  - ✓ House Web sites.
  - ✓ If a hacker can successfully attack a Web server, the Web server may not be able to function properly.
  - ✓ What would happen if Amazon.com or eBay.com went down for an entire business day?

What Devices are Usually Attacked? (cont'd)

- Computers
  - ✓ Computers can store confidential personal and corporate data.
  - ✓ If a hacker can gain access to this information, they might use it for personal gain, sell it to another party, or use it for blackmail purposes.

How do Hackers Attack Devices?

- Packet sniffers can read Internet traffic.
- Install malware.
  - ✓ Adware – Continuous ads on your screen.
  - ✓ Spyware – Reports on sites you visit.
- Guess at user names and passwords.
  - ✓ Don't use easy-to-guess passwords.
  - ✓ Do change default usernames and passwords (wireless routers).

Secure Your Operating System

- Install critical updates
  - ✓ For Windows operating systems (OS), critical updates fix security flaws and should be installed as soon as they are released.
  - ✓ Optional updates should not be automatically installed.
  - ✓ Only install optional updates if you determine that they are needed.

Secure Your Files

- Install anti-virus (AV) protection software
  - ✓ Commercial AV software is more robust than free AV software.
    - Will catch and quarantine almost all Trojan horse, virus, and worm attacks before they do any harm.
  - ✓ AV software works by recognizing "patterns" and stopping what it considers bad behavior.
    - Patterns should be updated daily to protect computer against new attacks.
  - ✓ If you decide to install more than one AV program on your computer, verify that they will work together before installation.
    - Some AV software do not work well together.

Engage in Safe Browsing

- When surfing never click on a popup unless you are absolutely sure of its owner
  - ✓ Some popups may indicate that the computer is infected with viruses and that you should click the popup to cleanse your system.
    - Never trust these messages. It is more likely that your AV software will locate and remove malware and viruses than a Web site's software.

Close Popup Windows Safely

- Press the key combination of ALT+F4 to terminate popups. This ensures that the popup will not install malware.
- Do not click anywhere on or in the popup window with your mouse. Clicking may install malware.

Secure Your Computer System

- Turn on a firewall
  - ✓ Firewalls permit or deny a computer the ability to connect to another computer.
  - ✓ The firewall will disable ports that should not be open and restrict use of ports to certain programs.

Manage Cookies

- A cookie is a text file that a Web site stores on your computer.
- Cookies cannot harm your computer.
- Web sites use cookies to keep track of your preferences and to record Web pages you visit.
  - ✓ First party cookies are placed on your computer by Web site owners. These are usually okay.
  - ✓ Third party cookies are placed on your computer by companies authorized by the Web site owner to place a cookie on your computer.
    - ➢ Some experts recommend accepting first party, rejecting third party, and allowing session cookies.

Manage Cookies (cont'd)

- Recommended settings in Internet Explorer…

Passwords and the Internet

- Use complex passwords:
  - ✓ At least six characters.
  - ✓ At least one upper-case character.
  - ✓ At least one number.
  - ✓ At least one symbol (# ! @ $ %, etc.).
  - ✓ Never use common information in a password.
- Do not write passwords on paper.
  - ✓ Hackers know to search around the monitor, keyboard, and general computer area to find passwords.

Know Who Uses Your Computer

- Utilize user accounts on your computer
  - ✓ Don't log in using the "administrator" account.
  - ✓ Tracks who has logged in and some of the things they do while logged in.
- Require all computer users to have their own user account and password.
  - ✓ Don't set up users as administrators.
- Set users as Power Users or Users to decrease the chances of them infecting your computer.

Other Internet Security Considerations

- Never use a public computer to conduct personal business.
- Use your personal computer with commercial, up-to-date AV software installed.
- Use strong passwords on all online accounts to prevent others from viewing or stealing your data.
- Always log out of any session you logged into before leaving the computer.
- Never open an e-mail from an unknown recipient.
  - Don't even click it once.
- Never open or save an e-mail attachment unless you know and trust the sender.

Trojans, Viruses, and Worms

- A Trojan horse is a malware program that usually impersonates a known good file installed on the system by replacing (deleting) the good file.
  - ✓ Gets its name from the Greek Trojan Horse myth.
  - ✓ The Trojan then does its dirty work on a certain date, through a user action, or on command.
  - ✓ Trojans can destroy or copy data, install adware, or install a browser toolbar.
  - ✓ Trojans can record keystrokes and send this to the attacker and scan computer ports.

Trojans, Viruses, and Worms (cont'd)

- A virus is computer program that can harm a computer and make it inoperable. Some viruses are only an annoyance.
  - ✓ Viruses usually do not replicate (make copies of) themselves on other computers.
  - ✓ Removing the virus usually cleans the computer.
  - ✓ Sending a virus via e-mail may replicate the virus.
  - ✓ In 2008, the Fun.exe virus spread itself via e-mail throughout the world and was very difficult to remove as it made many copies of itself on an infected computer.

Trojans, Viruses, and Worms (cont'd)

- Macro viruses usually infect Microsoft Office files and install themselves when users click files.
  - ✓ A macro is a small program, usually written in VBA (Visual Basic for Applications).
  - ✓ Macro viruses spread when users click files in which the macro virus resides.
  - ✓ Macro viruses may also delete files, etc. on an infected system.

Trojans, Viruses, and Worms (cont'd)

- A worm is a program that works to create a lot of network traffic.
  - ✓ Some worms are not malware as they crawl the network searching for reporting information.
  - ✓ Most worms replicate themselves, making the network unusable.
  - ✓ The ILOVEYOU worm successfully attacked millions of computers (users clicked the attachment) in May 2000.

Trojans, Viruses, and Worms (cont'd)

- Phishing
  - ✓ Phishing is an attempt to trick you into revealing personal information to an attacker so they can impersonate you.
  - ✓ Pronounced like the word "fishing," the attacker is fishing for information about YOU!
  - ✓ You may receive an e-mail that appears to be from your financial institution, eBay, or Amazon, asking you to login to verify a transaction.

Trojans, Viruses, and Worms (cont'd)

- ✓ When you click the link in the email, the Web site looks as you expect it to.
- ✓ No reputable organization will every ask you to do this.
- ✓ Report the attack to your organization so they are aware of the attack. Most companies will act on reported phishing attempts.

- Most e-mail software includes the ability to monitor for phishing and move the suspected e-mail to a non-functional (Junk e-mail) folder.

Trojans, Viruses, and Worms (cont'd)

- Hoaxes
  - ✓ Hoaxes are usually harmless and attempt to convince you of something that is not true.
  - ✓ Hoaxes usually come in the form of an e-mail.
  - ✓ Some hoaxes invite you to send money to someone in another part of the world, others ask you to contribute to find missing children, etc.
  - ✓ Use your search engine to determine whether the e-mail's message is true by entering the e-mail subject line in a search engine.
  - ✓ The result will usually indicate whether the email is a hoax.

Trojans, Viruses, and Worms (cont'd)

- Uncloak a Hoax
  - ✓ Use trusted Internet sites to detect hoaxes.
  - ✓ Snopes.com - http://www.snopes.com/.
  - ✓ Urban Legends Online - http://urbanlegendsonline.com/.
- Never forward e-mail chains without verifying their source.

Ethical considerations of the Internet

- Sharing Internet connection with neighbors.
  - ✓ Should neighbors have the ability to pool together, lease an Internet connection from an ISP, and pay for shared one connection?
- Downloading software from the Internet.
  - ✓ Should license “key generator” sites be allowed to operate?
  - ✓ Should people be able to download pirated software from the Internet?
  - ✓ Pirating software is a copyright infringement; selling unauthorized copies of commercial software, usually at a very low price.