



# COMPUTER-INTERNET SECURITY

How am I vulnerable?



# COMPUTER-INTERNET SECURITY

- ◆ Virus
- ◆ Worm
- ◆ Trojan
- ◆ Spyware
- ◆ Adware
- ◆ Messenger Service

# VIRUS



- ◆ A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user.
- ◆ A virus must meet two criteria:
  - ◆ It must execute itself. It will often place its own code in the path of execution of another program.
  - ◆ It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.



# VIRUS - DAMAGE

- ◆ Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages. Even these benign viruses can create problems for the computer user. They typically take up computer memory used by legitimate programs. As a result, they often cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.



# WHAT IS NOT A VIRUS

- ◆ It is easy to blame any computer problem on a virus. The following are not likely to be caused by a virus or other malicious code:
- ◆ **Hardware problems.** There are no viruses that can physically damage computer hardware, such as chips, boards, and monitors.
- ◆ **You have two antivirus programs installed and one of them reports a virus.** While this could be a virus, it can also be caused by one antivirus program detecting the other program's signatures in memory.

# WORMS



- ◆ Worms are programs that replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which requires the spreading of an infected host file.
- ◆ Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will then travel from computer to computer, so the entire document should be considered the worm.

# TROJAN



- ◆ Trojan Horses are impostor files
- ◆ Files that claim to be something desirable but, in fact, are malicious. A very important distinction from true viruses is that they do not replicate themselves, as viruses do.





# TROJAN - DAMAGE


- ◆ Trojans contain malicious code, that, when triggered, cause loss, or even theft, of data. In order for a Trojan Horse to spread, you must, in effect, invite these programs onto your computers -- for example, by opening an email attachment.



# SPYWARE



- ◆ Spyware is a generic term for a class of software designed to gather information. Although software of this type can be legitimate, it can, in some cases, be installed on your computer without your knowledge. This poses privacy concerns for many people.



# SPYWARE - PURPOSE

- ◆ The general purpose of spyware is to gather information about your Internet surfing habits and deliver that information to its customers.
- ◆ It can also gather information on the use of your personal computer and even the keystrokes entered into your computer's keyboard.



# SPYWARE – FORMS OF

- ◆ Spyware basically comes in, but is not confined to, three forms:
- ◆ As software bundled and installed with another software application,
- ◆ As a stand-alone installation package,
- ◆ As a modification to the HTML of a Web page.



# SPYWARE - DAMAGE

- ◆ Spyware programs, while they may be objectionable, are generally not malicious as far as damaging the computer. Most spyware programs have Web sites, and many of these sites have privacy statements or FAQs that explain what they do and what types of information they collect. This information can assist you in making an informed decision on whether to keep or uninstall the spyware.



# SPYWARE - NOTES

- ◆ In many cases, when the spyware is installed with a utility or game you downloaded, you may have to uninstall the utility or game to uninstall the spyware. If you uninstall only the spyware, the utility or game may become unusable.
- ◆ Spyware is often bundled with free downloadable Internet programs such as Web browsers, browser enhancements, desktop utilities, browser theme packages, and games.

# ADWARE

- ◆ Adware is a type of program that displays an advertisement of some sort, usually related to a specific Web site in your Web browser. In some cases, it changes the home page of your Web browser to point to a specific Web site.






# ADWARE - INSTALLATION

- ◆ In most cases, some user interaction is required to install adware. You must either double-click the program to run it, or there is information on the Web site to inform you that it will install a program on your computer. (This information may not be obvious, however.)
- ◆ Because adware programs are not generally malicious, and are not viruses, worms, or Trojans, Most AntiVirus programs do not detect them as such.





# ADWARE - DAMAGE

- ◆ Intrusion on “your computer” by an unknown third party,
- ◆ Annoying windows on desktop,
- ◆ Unwanted redirection to another website.



# MESSENGER SERVICE

- ◆ Operates over NetBIOS Ports – 135, 136, & 137
- ◆ All versions of Windows, and many other operating systems, use these ports in networking



# MESSENGER SERVICE - USES

- ◆ Most often used to deliver unwanted SPAM
- ◆ Often used to try to “scare” the computer user into purchasing a program to protect the user from “viruses, etc” by saying your computer is unprotected



# WHAT CAN I DO?

- ◆ Be aware of what is being installed on your computer,
- ◆ Don't automatically accept attachments in email,
- ◆ Disable "automatic download" in web browsers,
- ◆ Limit use of "JavaScript", "ActiveX" & "Windows Scripting Host" in your web browsers.
- ◆ Turn off the messenger service if not needed or use a firewall or router to block those ports

# WHERE CAN I GET MORE INFORMATION?



- ◆ Websites:

- ◆ <http://grc.com/su-bondage.htm>

- ◆ <http://www.staff.uiuc.edu/~ehowes/main.htm>



# WHERE CAN I GET MORE INFORMATION?

- ◆ Newsgroups:

- ◆ [news.grc.com](http://news.grc.com)

- ◆ Your ISP's newsgroup – i.e. 'news.tyler.net'

# HOW CAN I STOP THE INTRUSION?



- ◆ AntiVirus (software)
- ◆ AntiTrojan (software)
- ◆ AntiSpyware/AntiAdware (software)
- ◆ Router/Switch (hardware)
- ◆ Firewall (software or hardware)



# QUESTIONS ?

