

Grade Level: 9-12

Duration: One 15 minute session

Description: This lesson is designed to help students recognize and protect themselves against various forms of malware.

Content Outline:

1. Read, or have students read, the following: (adapted from: Hacker High School http://www.hackerhighschool.org/lessons/HHS_en6_Malware.pdf)

Viruses are self-replicating pieces of software that, similar to a biological virus, attach themselves to another program, or, in the case of “macro viruses”, to another file. The virus is only run when the program or the file is run or opened. It is this which differentiates viruses from worms. If the program or file is not accessed in any way, then the virus will not run and will not copy itself further. There are a number of types of viruses, although the most common form today is the macro virus.

A worm is a program that, after it has been started, replicates without any need for human intervention. It will propagate from host to host, taking advantage of an unprotected service or services. It will traverse a network without the need for a user to send an infected file or e-mail. Most of the large incidents in the press recently have been worms rather than viruses.

Trojans are pieces of malware which masquerade as something either useful or desirable in order to get you to run them.

Spyware consists of programs that collect data from a user or a computer and send it to someone else.

2. Have students brainstorm ways of protecting themselves from malware – list examples.
3. Compare your list to the following (adapted from IANAG Forums - <http://forum.networktechs.com/showthread.php?t=50>)
 - Be sure to visit Windows Updates often (at least once a month).
 - Make sure you are running a good Anti-Virus program, and keep it up to date.
 - A good firewall is absolutely mandatory. Windows XP comes with a built in firewall, but it only monitors incoming traffic.
 - Use strong spyware scanners and blockers.

- Be careful! Don't download files or install software unless you know they are safe. Don't open attachments you aren't expecting or from people you don't know.