Computer Viruses

Matthew Boulton College

COMPUTER VIRUSES

Norton Utilities: www.symantec.com
Mcafee Virus Detection: www.mcafee.com
Anti-Virus Resources:
http://members.tripod.com/lovegod11/bu1.html

Not so long ago, individual computer users could avoid virus infections without much thought or planning, simply because they rarely came in contact with likely virus sources. Today, however, most computer users send messages to each other, share data and transfer files constantly - whether through a modem, via diskettes, or over networks and the internet. In this same span of time, viruses have come to number in the thousands and spread more quickly and easily than ever.

In this environment, taking steps to protect yourself from a computer virus infection is no longer a luxury but a necessity. Consider the value of the data on your computer. It would probably require a significant investment of time and money to replace if it became corrupted or unusable because of a viral infection - it may even be irreplaceable. But whether your own data is important to you or not, neglecting to guard against viruses may mean that your computer could play unwitting host to a virus that can spread and attack the data on computers your co-workers and colleagues use.

Scheduling periodic virus scans significantly reduces your vulnerability to infection and prevents unnecessary loss of time, money and data.

What Is A Computer Virus
A computer virus is a program that replicates itself, attaches to other programs, and performs unsolicited or unwanted, if not malicious, actions when it executes. The two fundamental virus categories are “boot” and “file” viruses.

Boot viruses dwell in the boot sector of the hard or floppy disk that carries them. These execute as your computer starts. Once they copy themselves into your computer’s memory, they can then spread to other disks or other computers on a network, each time leaving copies of themselves that can repeat the cycle.

File viruses become active only when you execute the program that carries them. Typically, such viruses infect files with the extensions .EXE, .COM, or .DLL, and non-executable files such as Microsoft Word or Excel data and template files. Once executed, the file virus also loads itself into your computer’s memory, then replicates and attaches itself to other executable programs.

Virus Detection and Prevention Tips

1. Do not open any files attached to an email unless you know what it is. Some viruses can replicate themselves and spread through email.

2. Exercise caution when downloading files from the internet or opening files from an unknown source. Verify that an anti-virus program checks the files or disk. If you are uncertain, copy file to a floppy disk and test it with anti-virus software.

3. Using fonts that comes with client's files can be a source of viruses. These may have inadvertently picked up a virus from another computer.

3. Update anti-virus software regularly. Over 500 viruses are discovered each month. These updates should be at the least the products virus signature files. It may be necessary to update the product's scanning engine as well.

4. Back up files on a regular basis. If a virus destroys files, at least they can be replaced with the back-up copy. Store backup copy in a separate location from the work files, preferably on another computer.

QUESTIONS ON COMPUTER VIRUSES

(1) Give a definition of a computer virus?

(2) Name the 2 fundamental virus categories?

(3) Which virus sits in the boot sector of the hard or floppy drive?

(4) Describe how the ‘file’ virus works?

(5) When downloading files from an unknown source, give an example of a procedure for checking the file?

(6) Name a website address where information can be found on software for virus detection and removal?

(7) Describe how files from an unrecognised source are checked for viruses where you work?

(8) Describe how files are backed-up where you work, what is the frequency, what software is used and what storage device is used to store the copied files?