



FCC Computer Security Notice



COMPUTER SECURITY WEEK 2002

VIRUSES 101

Six or seven years ago, very few people were concerned about getting a computer virus. Perhaps, if you were sharing pirated software or were constantly transporting documents from work to home, it was an occasional nuisance.

What is a "Virus"? A virus is software which reproduces its own code by attaching itself to other software or to a document. Once attached, the virus code is executed without the consent or knowledge of the unsuspecting user.

Origins - People create viruses for a number of mischievous reasons. The most common reason is to bring attention to themselves or their cause. A person has to create the virus by writing the code, testing it to make sure it spreads properly, and then the virus is released.

The creator of the virus also determines whether the virus will attack by presenting a silly message or executing the destruction of your hard disk.

The most common types of viruses are:

Boot Sector Viruses - These viruses can spread through bootable CDs and floppy disks. Any disk can cause infection if it happens to be in the drive when the system boots up. The virus can also be spread across networks from file downloads and from e-mail file attachments. In most cases, write-enabled floppies used on an infected PC will pick up the boot sector virus.

Macro Viruses - These are collections of instructions to be carried out by a program or computer usually handling tasks that are boring, awkward, and tedious. In Word, macros can execute lists of instructions, reducing the number of keystrokes required to perform a given task.

Program Viruses - These are viruses which attach themselves to, or associate themselves with a file. File infectors usually append or pre-affix themselves to regular program files or overwrite program code. The file infector class is also used to refer to viruses that do not physically attach to files but associate themselves with program filenames, similar to Trojan horses.

E-mail Viruses - An e-mail virus spreads through other e-mail messages and usually replicates itself by automatically mailing itself to the other people in the victim's e-mail address book. E-mail viruses differ from "e-mail-borne viruses." All forms of viruses can be delivered via e-mail.

How Viruses are Detected - The primary means of defending against viruses is antivirus software. Antivirus software compares files on your PC with known virus profiles. These profiles are kept in what is called the virus signature files. As viruses are introduced, virus signature file need to be updated. These are usually obtained from the antivirus software manufacturer.

How to know your antivirus software failed - There are several ways in which viruses manifest themselves on your PC. The inability to boot your system or having it boot incorrectly is an indication that things may be rotten in Denmark. Other indications include unpredictable actions, degradation in computer response, excessive network utilization, and corrupted data.

Ways in which you can rid yourself of viruses with a few simple steps are:

Removing Boot Sector Viruses - (1) Antivirus software is the first line of defense; (2) Manually delete known virus files; (3) Clear the memory of your PC; (4) Wipe the boot sector; and (5) Wipe the hard drive clean.

Removing Macro Viruses - (1) Antivirus software is the first line of defense; (2) Manually delete known virus files; (3) Reinstall the application; and (4) Reinstall the operating system.

Removing Program Viruses - (1) Antivirus software is your first line of defense; (2) Manually delete known infected executable files and replacing them with clean versions; (3) Reinstall the operating system if the virus is spreading rampantly.

Removing E-mail Viruses - (1) Antivirus software is your first line of defense; (2) Delete the uninvited e-mail; (3) Clear the memory of your PC, and (4) Disconnect the computer from the network.



COMPUTER SECURITY TIP OF THE MONTH:

IT IS COMPUTER SECURITY WEEK HERE
AT THE COMMISSION. KEEP AN EYE OUT
FOR THE COMPUTER SECURITY WEEK
EVENTS ON THE NEWLY DESIGNED
COMPUTER SECURITY PROGRAM
WEBSITE.

YOU CAN REFERENCE ADDITIONAL INFORMATION ABOUT FCC COMPUTER SECURITY WEEK AT:

<http://intranet.fcc.gov/omd/itc/csg/index.html>