

Computer viruses

15326

[Technology](#), [Computer](#)



Computer Viruses A computer virus is an illegal and potentially damaging computer program designed to infect other software by attaching itself to any software it contacts. In many cases, virus programs are designed to damage computer systems maliciously by destroying or corrupting data. If the infected software is transferred to or accessed by another computer system, the virus spreads to the other system. Viruses have become a serious problem in recent years, and currently, thousands of known virus programs exist (Reed 85-102). Three types of viruses are a boot sector virus, file virus, and Trojan horse virus. A boot sector virus infects the boot program used to start the system. When the infected boot program executes, the virus is loaded into the computer's memory. Once a virus is in memory, it can spread to any floppy disk inserted into the computer. A file virus inserts virus code into program files. The virus then spreads to any program that accesses the infected file. A Trojan horse virus (named after the Greek myth) hides within or is designed to look like a legitimate program. Some viruses interrupt processing by freezing a computer system temporarily and then displaying sounds or messages. Other viruses contain time bombs or logic bombs. A time bomb is a program that performs an activity on a particular date. A logic bomb is a program that performs an activity when a certain action occurs, such as an employee being terminated. A worm, which is similar to a virus, copies itself repeatedly until no memory or disk space remains.

To detect computer viruses, antivirus programs have been developed.

Besides detecting viruses, antivirus programs also have utilities to remove or repair infected programs and files. Some damaged files cannot be repaired

and must be replaced with uninfected backup files. The table below outlines some techniques used to protect computer systems.

Techniques for Virus Protection and System Backup
Using Virus Protection Software
Backing Up Your System

Install virus protection software on every computer system. Develop a regular plan for copying and storing important data and program files. Before use, scan every floppy disk with a virus scan program to check for viruses. Implement a backup plan and adhere to its guidelines. Check all programs downloaded from the Internet or bulletin boards for viruses. Keep backup copies of files in fireproof safes or vaults or off-site. If your system becomes virus infected and you have questions, contact the National Computer Security Association (NCSA) for low-cost assistance (Elmhurst, 6 Nov. 1998). Works Cited Chambers, Anita R., and Zachary W. Peters. Protecting Against Virus Attacks. *Computers* May 1998: 45-62. Elmhurst, Mark. Virus Infection: Where to Obtain Assistance *Word* 97, Project 3. <http://www.scsite.com/wd97/pr3.htm> (6 Nov. 1998). Reed, Margaret E. *An Introduction to Using Computers*. Chicago: West Davidson Jones Publishing Company, 1998.