

Virus Scanner

Viruses can infect any computer and cause serious damage. A virus is a small program that, when it is inadvertently run, takes control of the infected computer. This gives the virus the opportunity to perform destructive actions, like deleting or writing over files or changing random bits of data.

Tip New viruses are continually being propagated, so it is important to stay informed and to keep your Safe & Sound software updated. Network Associates' Internet website offers a wealth of excellent information about computer viruses, including antivirus technical support; a Virus Info Library that defines individual viruses, hoaxes, research, and technical information; and White Papers that describe viruses and the countermeasures you can take to combat them. To access this information, point your web browser to:

<http://www.nai.com/vinfo/>

What is a Virus?

A *virus*, like its biological namesake, replicates itself and attaches to another program, or any file that can be run (such as a word processing or spreadsheet macro). When you run the infected program or macro, you unknowingly run the virus.

While the virus is running, it has the opportunity to clone itself, thus spreading from one disk or drive to another; it also has a chance to damage or destroy your valuable information.

Anyone can write a computer virus, even people who are not programmers, so viruses can either do no damage at all or far more damage than intended. Few viruses are written to be destructive, but the simple fact that a virus takes control of your computer—sometimes as soon as you start your computer—makes viruses a serious threat. Worst of all, if even a single copy of a virus remains “in the wild” (that is, lying dormant on anyone’s computer without their knowledge), then it may be able to quickly spread from one machine to another.

How Are Viruses Transmitted?

Any software interaction with another computer gives a virus a possible entry point to your system. The most common method of getting a virus is from an infected disk, such as when you install software from either 3.5-inch disks or CDs. Software manufacturers check for viruses when creating *golden masters* (the master disk set

used for creating all other copies of their software). This does not mean that they will always detect and clean every virus. A new virus could easily evade detection, or one disk might be accidentally missed in the virus scanning process.

Furthermore, viruses can be designed to avoid detection in a number of ways. Viruses are written, with varying degrees of success, to hide from detection when examined using standard file handling software (such as My Computer or Windows Explorer). For example, when a virus clones itself, it can save a copy of the information it overwrites including file size, creation and modification dates, and so on. When Windows Explorer attempts to read this information, these viruses (called *stealth* viruses) simply supply the pre-infected information. This means that you cannot always tell whether your computer has a virus just by checking program information to watch for sudden changes.

Your computer can also become infected when you connect to another computer via modem (direct, Internet, BBS, or online service connections) or any form of network connection. A virus can be copied to your machine, but until you perform the action that triggers that virus, it stays inactive. A trigger event could be running the program the virus has attached itself to, a particular date or time, or even certain characters you type.

What Types of Viruses Can I Encounter?

There are three major categories of viruses: boot sector, file and macro. Safe & Sound's Virus Scanner checks for all of these types of viruses.

Boot Sector Viruses

Boot Sector viruses copy themselves to the boot sector of a disk. The *boot sector* is the first sector on a disk that contains special information used to startup (or boot) your computer. A boot sector virus gains control of your computer from the moment you start your machine. Typically, this virus becomes resident in your computer's memory the same way Bomb Shelter does when it is active.

Tip Bomb Shelter does protect certain critical areas of your computer's RAM from being overwritten by applications (including virus programs). However, it is aimed at securing your system against system crashes rather than against virus attacks.

File Viruses

To perform any action, a virus must be run. With this in mind, a file virus attaches itself to a file it knows can be run, which includes COM,

EXE, SYS or BAT files. File viruses sometimes also attach themselves to OVL or OVI overlay files. Once the virus is attached to a file, it will be run the next time you start that program or run the macro. When this happens, the file virus can propagate itself and cause damage to your computer's information.

File viruses are the most common type of virus, but because they overwrite part of the original program, they usually cause the program to fail in some way. This provides a warning signal that makes file viruses easier to detect.

Macro Viruses

Macro viruses take advantage of the power of macro languages offered by application programs, such as Microsoft Word or Excel. A macro virus uses macro commands to perform undesirable actions on your computer when they are run from within the application that supports them. It doesn't take a programmer to write a macro virus.

Externally, a macro virus looks like a regular document, and until recently, regular documents were considered safe from virus infections. This means that macro viruses can spread very quickly.

Logic Bombs, Trojans, and Worms

There are other kinds of programs that can be written to damage your computer, but that are not viruses because they either cause damage but do not replicate themselves, or vice versa.

A *logic bomb* is a program that stays on your computer and remains inactive until some trigger event. When that trigger takes place, the logic bomb performs some destructive action. For example, a logic bomb might be copied to a computer by a disgruntled employee. The logic bomb has a particular target and does not clone itself.

A *trojan*, like the trojan horse which is its namesake, delivers a destructive program (a logic bomb or virus). A trojan goes in the guise of an attractive, or seemingly useful program (such as a game or utility program).

A *worm* is a program whose sole purpose is to clone itself, without taking any other form of destructive action. By itself, a self-replicating program can bring a computer or even a network to a standstill by stealing exponentially increasing amounts of CPU time and storage space.

How Can You Combat Viruses?

Virus Scanner checks for viruses in your computer's memory, in the boot sector, and in files. It does this using a sophisticated, algorithmic checking process. Simply start Safe & Sound and click the Virus Scanner button. Follow the instructions on your screen and Virus Scanner examines your computer's memory, boot sector and files for viruses. If it finds them, it gives you a report and clears them from your system.

Thereafter, you should also follow some preventive guidelines to help ensure that viruses have a more difficult time gaining access to your computer. For example, you should write-protect the disks you use whenever possible.

Also, you should only run a macro when you know exactly where it came from and who created it.

Recovering From a Virus Attack

Once a virus has already attacked your system, Virus Scanner cannot perform the kind of repairs that may be necessary. To help you repair a damaged computer, run Safe & Sound's System Checker or Disk Minder for DOS.

If the virus has deleted files from your drive, you may need to recopy these files from your latest backup set.

If the damage to your drive is severe, you may need to reformat the drive and reload your latest complete backup set. As soon as you finish this process, be sure to rerun Virus Scanner to catch the virus before it has a chance to destroy your data again.

If none of these things work, you can contact Network Associates' Technical Support department for assistance with your particular virus and how to recover from the attack. Late-breaking information is also offered at the Network Associates' <http://www.nai.com/> website.