Using 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.

Note 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/

These topics explain viruses and why you need to use Virus Scanner:

- What is a Virus?
- How Are Viruses Transmitted?
- What Types of Viruses Can I Encounter?
- Logic Bombs, Trojans, and Worms
- How Can You Combat Viruses?
- Recovering From a Virus Attack

To scan your PC for viruses:

1. Click the Start button and do one of the following:
   - Choose the Safe & Sound command from the Start menu and click the Virus Scan button.
   - Choose the Programs > Safe & Sound > Virus Scanner command.

   The Virus Scanner window appears.
2. Select the tests you want to perform and click Next >.

   Virus Scanner performs the tests you selected. It displays a progress thermometer to let you know how the process is going. If it finds any viruses, it lets you know. For information about what to do next, see Recovering From a Virus Attack.
3. Click Finish.

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 (even shrink-wrapped 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.

Note 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 of them so that you can clear them from your system. For more information, see Recovering From a Virus Attack.

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 Retake 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.

Virus Scanner Window

The Virus Scanner window lets you select the areas of your system that you want to scan for viruses. If it finds a virus, it lets you know so that you can begin the recovery process. For more information, see Recovering From a Virus Attack.

Memory
Virus Scanner checks your physical memory (RAM, or random access memory) for viruses.

Boot Sector
Virus Scanner checks for Boot Sector viruses which copy themselves to the boot sector of your computer's hard drive. These virus programs are TSRs (Terminate Stay Resident programs) that load when you start your PC. They take control of your computer as soon as you start it.

Files
Virus Scanner checks all the files stored on your hard drives for viruses.

Floppy Drive (A:)
Virus Scanner checks the 3.5-inch disk in your floppy drive for viruses. It checks the disk's boot sector and files.

Next > / Finish
Until you finish scanning for viruses, this button is titled Next >. Click the Next > button to begin scanning your PC for viruses.

Once the virus scan is complete, this button is titled Finish. Click the Finish button to exit Virus Scanner.

Cancel
Click the Cancel button to close Virus Scanner without finishing the virus scan.

< Back
Click the < Back button to go back and select different areas of your PC system to scan for viruses.

Address Space

The sum total of all possible memory addresses available at a given time. This is 4 GB (gigabytes) on a 386 or later PC in protected mode.

Launch Pad

The Launch Pad is a window where you can place application and document icons so you can conveniently access them.

Benchmarks

A benchmark is a standardized task that tests various devices for measurements, such as speed.

BIOS

The BIOS (or Basic Input/Output System) contains buffers for sending information from an application to the hardware device, such as a printer, where the information should go.

Buffers

A buffer is a temporary storage location for information being sent or received.

Bytes

A byte is eight bits of information composed of zeros and ones, one of which may be a parity bit. Most character sets, such as ASCII, use one byte to represent each character (letter, number, or special symbol).

Cache

A cache is part of the computer's memory used to temporarily store recently accessed information. A cache is designed on the premise that recently used information may be needed again soon. Keeping information available in cache reduces the time it takes for an application to obtain the information again.

Cluster

A cluster is a unit of storage allocation usually consisting of four or more 512-byte sectors.

Conventional Memory

Conventional memory is the first 640 K (kilobytes) of RAM (random access memory).

CPU (Central Processing Unit)

The “brain” of your computer. This is main computer chip that controls all activity that takes place on a computer.

Diagnostics

Diagnostics are tests run to detect faults in a computer system. Diagnostics tests are run to detect faults before they become serious problems so the faults can be corrected.

Directories

Directories are locations within a volume on a drive where you can store files or subdirectories. In Windows, directories are equivalent to folders that appear on the desktop in a drive window.

Discardable Memory

Discardable memory is memory used by an application that it has marked as discardable. Windows can reallocate the discardable memory to a different application if it needs to.

DLLs (Dynamic Link Libraries)

A DLL is an executable code module that can be loaded on demand and linked at run time. DLLs can be shared among multiple applications and independently updated, transparent to the applications. DLLs can also be unloaded when they are no longer needed.

DMA (Direct Memory Access)

DMA is a fast method of moving information from a storage device or LAN interface card directly to RAM which speeds processing time. DMA is direct memory access by a peripheral device that by-passes the CPU to save time.

Expanded Memory

DOS running on the Intel 80286, 80386, or 80486 family of computers can only address one megabyte of memory at one time. Expanded memory is the memory located between the base memory (either 512 K or 640 K) and one megabyte. Expanded memory is reserved by DOS for housekeeping tasks, such as managing information that appears on the screen.

Extended Memory

Memory above one megabyte in 80286 and higher PCs. Extended memory can be used for RAM disks, disk caches, or Windows, but it requires the CPU to run in a special mode (protected mode or virtual real mode).

FAT (File Allocation Table)

The FAT is an index to the location where all the information is stored on a floppy disk or hard drive. The FAT is extremely important because the system uses it to store and retrieve files containing information.

GDT (General Description Table)

The GDT is a table that is basic to the operation of protected mode. This table contains data structures (descriptors) that describe various regions of memory and how they may be accessed. Windows uses the GDT for system devices. *See LDT.*

Global Heap

The Global Heap is the general pool of memory available to Windows applications.

GPF (General Protection Fault)

An error condition caused by an application when it attempts to perform an operation not allowed by the operating system. Windows uses GPFs to determine and control the state of the currently executing application. GPFs that are unexpected by Windows cause a system error message to appear.

HMA (High Memory Area)

The HMA is the first 64 K of extended memory. If you use DOS 5.0, you can save memory by loading DOS into the HMA. Do this by adding the DOS=HIGH setting to your CONFIG.SYS file and restarting your PC.

Interrupt

A temporary suspension of a process caused by an event outside that process. More specifically, an interrupt is a signal or call to a specific routine. Interrupts allow peripheral devices, such as printers or modems, to send a call to the CPU requesting attention.

I/O (Input/Output) Device

An I/O device is any piece of computer hardware that can exchange information with the CPU. Examples of I/O devices include network cards, printers, speakers or other sound devices, or devices connected to the serial or parallel ports of your PC such as external modems.

Kernel

The Kernel is the part of a computer operating system that performs basic functions such as switching between tasks.

LDT (Local Descriptor Table)

The LDT is a secondary data structure table that contains additional information about various regions of memory and how they can be accessed. Windows uses the LDT for programs.

Linear Memory

Linear memory is the currently defined address space of the system that Windows uses to allocate memory to Windows applications.

Local Heap

The Local Heap is a region of memory allocated for local use by an application.

Locked Memory

Locked memory is memory used by an application that cannot be relocated or discarded by Windows.

Mapping

Mapping is the process of assigning physical memory (RAM) to a particular linear address range.

Mode Switch

A mode switch is a transition made by the CPU when changing from one mode of operation to another. For example, switching from real or protected mode, or a transition between different levels of protection. *See Ring 0, 1, 2, 3*.

Modules

A module is a device driver loaded by Windows.

Paging

The process of saving information stored in RAM to the swap file on the system hard drive so Windows can make the RAM available at a different linear address.

Parallel Port

The parallel port is a connector on the back of your PC and on some peripheral devices. With the appropriate driver software installed and a parallel cable connected to the parallel ports on your PC and a peripheral device, the two can communicate with each other. Parallel transmissions have no EIA standard, but most equipment follows a quasi-standard called the Centronics Parallel Standard.

PCI (Peripheral Component Interconnect) Bus

The PCI Bus is a local motherboard specification (that provides connector slots on the motherboard for installing peripheral cards). The PCI Bus, designed by Intel, offers a high performance, peripheral component level interface to the CPU bus.

Physical Memory

Physical memory is the RAM (Random Access Memory) installed in your PC. *See Random Access Memory (RAM).*

Protected Mode

A mode of operation of 80286 or later CPUs which allows access to more than 1 MB of memory.

RAM (Random Access Memory)

RAM (Random Access Memory) is also called physical memory. It is installed in your PC on SIMMs (Single Inline Memory Modules) or DIMMs (Dual Inline Memory Modules). RAM is volatile, extremely high-speed storage used by your computer for processing information.

Real Mode

A mode of 80286 or later CPUs, where the CPU operates substantially like an older 8086 CPU and can address directly only 1 MB of memory.

Resources

Resources are objects that Windows and its applications can use, such as the buttons on the screen that you can click.

Ring 0, 1, 2, 3

Different levels of protection in protected mode, where programs having varying degrees of freedom of operation. Ring 0 (zero) is least protected and has direct access to all hardware in the system.

Sector

A sector is a pie-shaped portion of a hard disk. A disk is divided into tracks and sectors. Tracks are complete circuits and are divided into sectors. Under DOS, a sector is 512 bytes.

Serial Port

A serial port is an input/output port (connector) that allows the transmission of information out at one bit at a time, as opposed to parallel which transmits eight bits, or one byte at a time.

Swap File

The swap file is created by Windows on the system hard disk. It uses the swap file to copy information stored in part of the linear address space so it can reallocate the RAM used at that location to another linear address space.

Swapping

Swapping is the process of saving to disk or restoring from disk the contents of RAM so that the RAM can be used elsewhere in linear memory.

System Resources

System resources are a series of data structures kept by Windows. System resources are managed by the Windows User and GDI programs and maintain information about objects that appear on your screen.

32BDA (32-Bit Disk Access)

32BDA is a process in Windows where the device driver that accesses the disk runs entirely as a 32-bit program at Ring 0 (zero).

32BFA (32-Bit File Access)

32BFA is a process in Windows where the DOS file operations are controlled by a program, or set of devices, that operate entirely as 32-bit programs at Ring 0 (zero).

Unlocked Memory

Unlocked memory is physical memory that Windows can copy to the swap file on disk, and whose linear address can be changed whenever Windows chooses.

UMB (Upper Memory Block)

The UMB is the area in memory between 640 K and 1 MB that have RAM mapped into them by memory managers, such as Network Associates' Netroom or MemMaker. *See Expanded memory.*

V86 Mode (Virtual 8086 Mode)

V86 mode is a mode of operation of 80386 or later CPUs where programs, originally designed to run in real mode, can run as sub-programs to a protected mode control program or operating system.

Video Memory

Video memory, called VRAM, is physical memory installed on your PC's video card that is used for displaying information on the screen.

Virtual Memory

Virtual memory is the amount of memory that exists either as physical memory (RAM) or on the hard drive (in the swap file). When a part of memory that is located in the swap file is accessed by an application, Windows reads the information into RAM.

VMs (Virtual Machines)

Virtual machines (also called Virtual DOS machines or VDMs) are created in Windows 95/98 when you open a MS-DOS Prompt window. The VDM is a software emulation of a separate computer, offering all the services that the DOS application expects of a PC.

VxDs (Virtual Device Drivers)

VxDs are used in Windows to communicate with all physical hardware in the system. This prevents any application from having direct access to a piece of hardware. Instead, it communicates only through the VxD for that hardware.

Windows Registry

The Windows 95/98 Registry file contains user, application, and computer-specific configuration information in a central location that was kept in various .INI files in Windows 3.1. The Registry contains settings that determine how your computer runs.