Computer Viruses and Their Control

Presented by Noel Bryson

September 18, 2000

What is a computer virus?

Computer viruses are executable computer programs. Like biological viruses, they find and attach themselves to a host. Just as a cold virus finds and attaches itself to a human host, a computer virus attaches itself to an item, such as a computer startup area (boot record) or an executable file.

Most viruses stay active in memory until you turn off your computer. When you turn off the computer you remove the virus from memory, but not from the file, files, or disk it has infected. So, the next time you use your computer the virus program is activated again and attaches itself to more programs. A computer virus, like a biological virus, lives to replicate.

Viruses are categorized by their infection targets:

Program viruses infect program files, which commonly have extensions such as .COM, .EXE, .SYS, .DLL, .OVL, or .SCR. The most common programs targeted by viruses are standard DOS programs that use the .COM and .EXE file extensions. Program files are attractive targets for virus writers because they are widely used and have relatively simple formats to which viruses can attach.

Boot viruses infect the non-file (system) areas of hard and floppy disks. These areas offer an efficient way for a virus to spread from one computer to another. Boot viruses have achieved a higher degree of success than program viruses in infecting their targets and spreading.

Macro viruses infect data files with macro capabilities and are the newest threat to the computing public. For example, Microsoft Word document and template files are susceptible to macro virus attacks. They spread rapidly as infected documents are shared on networks or downloaded from Internet sites.

All computer viruses fall into two groups:

Known viruses: A known virus has been identified. Symantec engineers work around the clock tracking reported outbreaks of computer viruses to identify new viruses. Once identified, information about the virus (a virus signature) is stored in a virus definitions file. When Norton AntiVirus scans your disk and files—initiated from the Scan For Viruses page of the main window or scheduled to run automatically—it is searching for these telltale signatures. If a file is found that has been infected by one of these viruses, Norton AntiVirus has the tools to eliminate the virus automatically.

Each time a new virus is discovered, its virus signature must be added to the virus definitions file by the Symantec engineers. For this reason, you need to update your virus definitions file regularly. Symantec has made this easy with the automatically scheduled Live Update feature.

Unknown viruses: An unknown virus is one that does not yet have a virus definition. Norton AntiVirus includes an advanced heuristic technology called Bloodhound to detect unknown program and macro viruses. Bloodhound isolates and locates the various logical regions of a file and then analyzes the program logic for virus-like behavior. Bloodhound detects a very high percentage of unknown viruses. In addition, Norton AntiVirus detects unknown viruses by monitoring activity on your computer for behaviors that viruses typically perform. When a suspicious activity is detected, Norton AntiVirus prevents the action from continuing.

Controlling Viruses

Software such as *Norton AntiVirus 2001,* which has an improved live update feature currently protecting against 47,720 viruses, and *McAfee* cost in the range of $39. These programs are also available in suites, which bundle several computer programs together.

Introducing Norton AntiVirus

When you install Norton AntiVirus and accept the preset options, your computer is safe. As part of the installation, your computer is scanned for viruses.

Norton AntiVirus automatically checks boot records for viruses at system startup, checks programs for viruses at the time you use them, scans all local hard drives for viruses once per week, and monitors your computer for any activity that might indicate the work of a virus in action. It also scans files you download from the Internet and checks floppy disks for boot viruses when you use them.

With Norton AntiVirus, you can scan files, folders, or entire drives for viruses, and quarantine infected files for submission to the Symantec AntiVirus Research Center (SARC). Files submitted to SARC are analyzed and the results are reported automatically within seven days.

Tasks you can perform with Norton AntiVirus
The list below shows the most important tasks Norton AntiVirus helps you perform.

- Scan for viruses on your computer.
- Remove viruses from your computer.
- Update your virus protection with LiveUpdate.
- Quarantine an infected file.

How Norton AntiVirus works
The scanner, which examines program files for the signatures of known viruses, is the heart of Norton AntiVirus protection. It searches for virus signatures when you initiate manual scans, when you schedule scans to run at specific times, during startup scans that run automatically every time you start your computer, and by the Auto-Protect feature every time a file is used. The scanner also verifies that boot records protected by inoculation have not been altered.

Manual scans
Use the Scan Now button in the Norton AntiVirus main window to initiate manual scans. These scans detect known viruses in specific files, folders, or drives on your computer.

Scheduled Scans
Scheduled scans are manual scans that run automatically at predetermined times. These scans supplement other automatic protection features to ensure that your computer is virus-free. As part of the Norton AntiVirus installation, a scan of your computer is scheduled to run automatically once per week.

To schedule virus scans:
1 Click Scheduling in the Norton AntiVirus main window.
2 Click New Event.
3 On the first page of the Scheduling wizard, click Next.
4 Select Schedule A Virus Scan.
5 Click Next and select the desired scan task from the list. If you do not see the scan task you want to schedule, you will need to define a new task.
6 Click Next and enter a brief description in the Description text box. This text appears in the Events list box in the Scheduler main window.
7 Click Next and select how often you want the scan to occur.
8 Click Next and enter the time and date when you want this event to first run.
9 Click Next, then click Finish.
NOTE: The Scheduler must be loaded in order to execute the scans you have scheduled.

Startup Scans
The first wave of defense against virus attacks are special scans that occur automatically each time your computer starts up. These scans catch viruses that infect the files and boot records your computer uses to ready itself for work. Startup scans are a vital part of virus protection because they make sure that your computer is virus-free each time you start it up. The startup scan is turned on during installation, unless you specifically turn it off.

Auto-Protect
Auto-Protect, the Norton AntiVirus automatic protection feature, scans program files, documents, and document template files for viruses whenever they are used. Auto-Protect, in addition to checking files for known viruses, uses Bloodhound technology and virus-like activity monitors (such as an attempted format of a hard disk) to make sure that unknown viruses are neither infecting your computer nor damaging data during the course of normal operation. Auto-Protect is already turned on after installation, unless you specifically turn it off.

About Norton AntiVirus Auto-Protect

Auto-Protect works in the background to protect you in several ways:

- Detecting viruses that may already exist and removing them.
- Preventing viruses from infecting your computer.
- Monitoring for activity that may indicate an unknown virus.

In addition to the scans that Auto-Protect performs in the background, you can also initiate scans at any time and schedule scans to occur at predetermined times.

To enable Auto-Protect:

1 Right-click the Norton AntiVirus icon in the lower right corner of the taskbar on your Windows desktop.

2 Click Enable Auto-Protect.

The button changes to Disable Auto-Protect and the icon changes.

NOTE: Norton AntiVirus is preset to enable Auto-Protect whenever you start your computer.

To disable Auto-Protect temporarily:

1 Right-click the Norton AntiVirus icon in the lower right corner of the taskbar on your Windows desktop.

2 Click Disable Auto-Protect.

The button changes to Enable Auto-Protect and the icon changes.

Inoculation

Once your disks are scanned to verify that they are free of viruses, Norton AntiVirus inoculates boot records to makes sure they stay virus-free. When a boot record is inoculated, Norton AntiVirus records critical information about it (similar to taking a fingerprint) in a special file designed specifically to store this inoculation data. On subsequent scans, Norton AntiVirus compares the current fingerprint to its stored fingerprint. You are alerted if there are any changes that could indicate the presence of a virus. Boot records are inoculated automatically as part of your Norton AntiVirus installation.

Virus definitions files

Virus definitions files contain information that Norton AntiVirus uses during scans to detect known viruses. Norton AntiVirus depends on up-to-date information. Each time a new virus is discovered, its virus signature must be added to a virus definitions file. You should update your virus definitions files at least once per month so that Norton AntiVirus has the information it needs to find all known viruses. New virus definitions files are available from Symantec regularly. If you have a modem or an Internet connection, Norton AntiVirus can update your virus definitions files for you automatically.

E-Mail Scan

Scans e-mail automatically as it is received detecting viruses in attachments before the user accesses the attachment eliminating risk of unknowingly forwarding viruses to others.

NOTE: For maximum protection schedule scans weekly and live updates monthly. Scan floppies before using by going to *main page*. Then select *drive*. Click *scan*.

To use Norton AntiVirus:

1 Double-click the Norton AntiVirus icon on the Windows taskbar in the lower right corner of the desktop to open Norton AntiVirus.

2 From the Norton AntiVirus main window you can view the current status of your system; initiate manual scans of selected files, folders, or drives; run the Norton AntiVirus Quarantine program; and schedule regular virus scans.

About Norton AntiVirus

This window gives subscription and expiration dates.

Norton AntiVirus Main Window For System Status

The Norton AntiVirus main window with System Status selected lets you get information about virus protection on your system:

- The status of Auto-Protect is displayed. It is recommended that Auto-Protect always be enabled so that it can check for viruses while running in the background. Click the Disable/Enable button to turn off or on the Auto-Protect feature.
- The list box contains several lines of status information. Each line contains a brief statement. You can select a line and click Details to get more information.

The Norton AntiVirus main window organizes the principle AntiVirus features into four groups. In addition to System Status you can:

- Click Scan for Viruses to run predefined scans or define new scans for later use. Predefined scans are listed in the text box.
- Click Reports to view Norton AntiVirus activity logs or use the Quarantine function to isolate infected or suspicious files for submission to Symantec AntiVirus Research (SARC).
- Click Scheduling to set up a scheduled scan to run when it is convenient for you.

You can also click any of the top buttons to help you better take advantage of Norton AntiVirus features:

- Click LiveUpdate to automatically update virus definitions and program updates.
- Click LiveAdvisor to connect to Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register.
- Click Rescue to create either a Zip Rescue disk or a set of rescue floppy disks.
- Click Options to customize Norton AntiVirus features.
- Click Help to get more information about the window you are viewing.

To get Help for many options in the Norton AntiVirus main window, position the cursor over the option, right-click, and choose What's This?

NOTE: You can keep help open on your desktop by minimizing the help window or by clicking back and forth between help and the product. When you have read the information you need, click in the open Norton AntiVirus window. Then, if you need help again, reopen help by clicking it in the taskbar below or by clicking in the help window itself.

To update virus definitions using LiveUpdate:

1 In the Norton AntiVirus main window, click LiveUpdate.

2 In the How Do You Want To Connect drop-down list box, select one of the following:

- Find Device Automatically: Norton AntiVirus determines if you have an Internet connection or must connect using your modem.
- Internet: Norton AntiVirus connects to the Symantec FTP (File Transfer Protocol) site on the Internet.
- Modem: Norton AntiVirus dials a preset number and connects to a Symantec server through your modem.

NOTE: Be sure that you enter any dial-out code (for example, 9) if one is required. However, do not enter a 1 for long distance.

3 Click Next to start the automatic update.

The new virus definitions files are automatically installed and take effect after you restart your computer.

NOTE: If you don't have a modem or access to the Internet, you can order virus definitions update disks from Symantec to arrive by mail from Symantec. This service requires a fee. Consult the Customer Service help page for applicable Symantec phone numbers.

Much of this information was re-printed from the Help Files of Norton AntiVirus 2000.