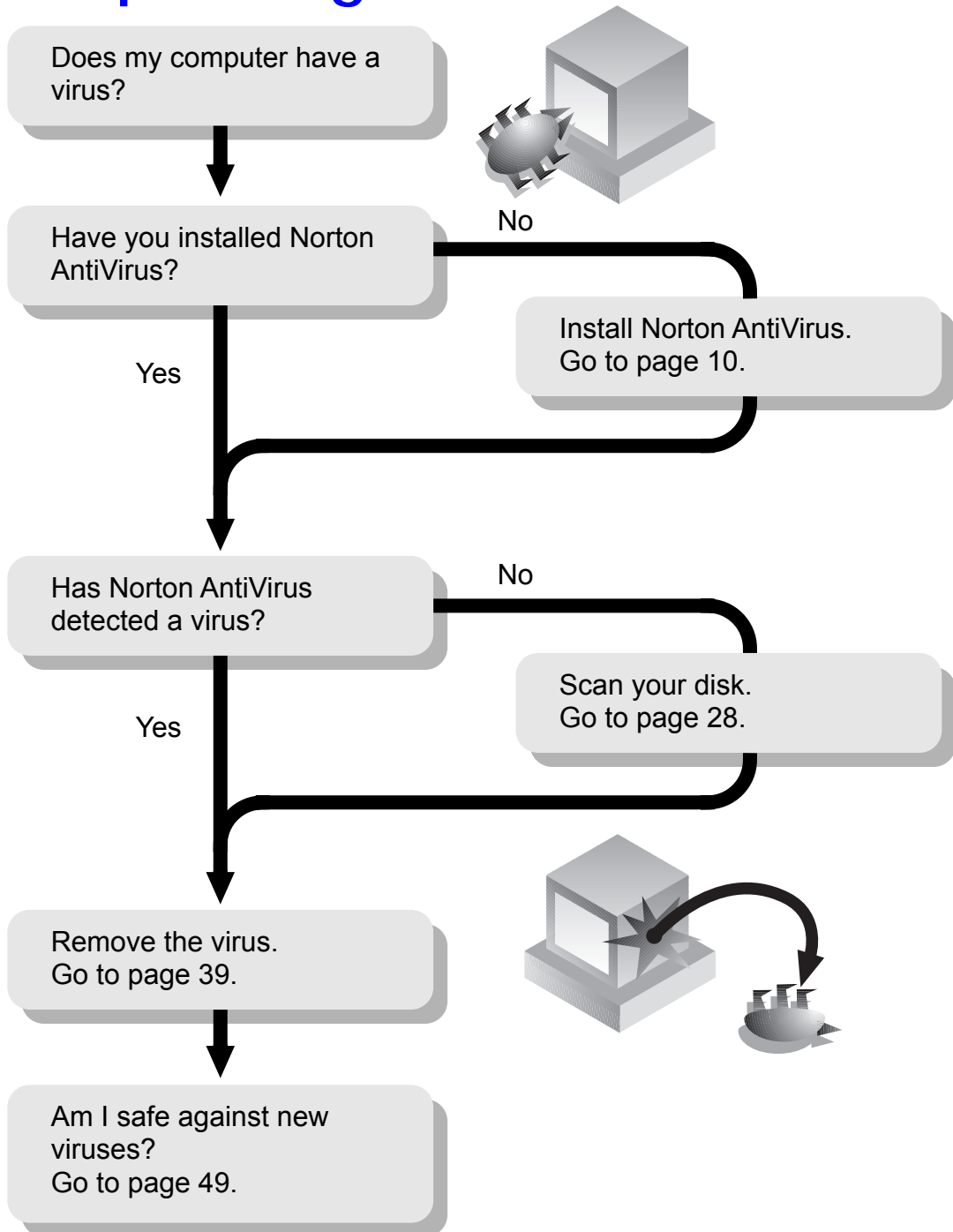


Reference Guide

NORTON

AntiVirus VERSION 5.0 TM

Help! I've got a virus!



Norton AntiVirus[™] for Windows[®] NT

Reference Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 1990-1998 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Trademarks

Symantec, Norton AntiVirus, Norton AntiVirus for Macintosh, and Norton Utilities are trademarks of Symantec Corporation.

Windows is a registered trademark and Windows 95 is a trademark of Microsoft Corporation. NetWare is a trademark of Novell Corporation. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

- You may:

- (i) use only one copy of one version of the various versions of the Software contained on the enclosed CD-ROM on a single computer;

- (ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;

- (iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;

- (iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and

- (v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

- You may not:

- (i) copy the documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software;
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
- (iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

- Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

- Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

- Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

- U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

- General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 10201 Torre Avenue, Cupertino, CA 95014.

C O N T E N T S

Installation

What Norton AntiVirus does automatically	9
What you have to do	9
Installing Norton AntiVirus for Windows NT	10
Installation requirements	10
Installing	10
Questions when installing	11
Uninstalling Norton AntiVirus	12

Chapter 1 About Norton AntiVirus

Is my computer protected against viruses?	13
What is a computer virus?	14
Virus infection cycle	14
How Norton AntiVirus protects you	16
Manual scans	16
Scheduled scans	16
Auto-Protect	16
Virus Definitions Files	17
Quarantine	17
How Norton AntiVirus warns you	17
Virus risk under Windows NT	19
Boot viruses	19
Program viruses	20
Macro viruses	20
Security considerations	21
MS-DOS and Windows NT	22

Chapter 2 Using Norton AntiVirus

Tips to avoid viruses	23
Starting and exiting Norton AntiVirus	24
Getting help	25
Scanning for viruses	25
Bypassing boot record scans	28
Scheduling virus scans	29
Enabling and disabling Auto-Protect	32
Viewing the Activity Log	34

Internet protection	35
Netscape and Norton AntiVirus	36
Other Internet Browsers and Norton AntiVirus	36

Chapter 3 Eliminating viruses

Eliminating viruses detected during scans	39
Command buttons	42
Eliminating viruses detected by Auto-Protect	43
What to do if repair is unsuccessful	45
Unable to repair a file	45
Unable to repair a system file	45
Unable to repair a boot record	45
Removing viruses from compressed files	46
Dealing with common problems	46

Chapter 4 Keeping up with new viruses

Automatically updating virus definitions	49
Using LiveUpdate Email	51
Scheduling an automatic LiveUpdate	51
Manually updating virus definitions	53
Viewing the Virus List	53

Chapter 5 Customizing Norton AntiVirus

Customizing manual scan options	57
Scanning network drives	62
Selecting which files to scan	62
Specifying program file extensions	63
Managing exclusions	65
Customizing alerts	67
Sending network alerts	68
Customizing the Activity Log	69
Setting backup options	70
Customizing automatic protection	71
Auto-Protecting program files	71
Auto-Protecting floppy disks	74
Setting password protection	74

Chapter 6 Managing the Quarantine

Using the Quarantine	77
Adding a file to the Quarantine manually	79
Submitting a file to SARC for analysis	79

Treating compressed files in the Quarantine	80
Configuring the Quarantine	81

Appendix A About computer viruses

What are computer viruses?	84
Virus targets	86
Program viruses	86
Boot viruses	87
Macro viruses	88
Virus technologies	89
Keeping your protection current	91

Appendix B Emergency recovery

When you can't start your computer	93
--	----

Appendix C Using command-line switches

Glossary

Index

Installation

Norton AntiVirus safeguards your computer from virus infection, no matter what the source. You are protected from viruses that spread from hard drives and floppy disks, those that travel across networks, and even those that are downloaded from the Internet.

What Norton AntiVirus does automatically

- Eliminates viruses and repairs files.
- Makes sure your computer is safe from viruses at startup.
- Checks for viruses every time you use software programs on your computer, floppy disks, or document files that you receive or create. (For example, the newest kind of viruses are spread via Microsoft Word and Excel macros.)
- Monitors your computer for any unusual symptoms that may indicate an active virus.
- Runs a scheduled scan automatically once per week to confirm that your hard disks are virus-free.
- Protects your computer from Internet-borne viruses.

What you have to do

To update virus protection, see page 49.

- Once a month, obtain from Symantec updated information that Norton AntiVirus needs to keep your virus protection up-to-date. You can do this online (for example, over the Internet) or by mail.

New viruses are being written all the time. You have to regularly obtain files from Norton AntiVirus that contain the latest virus protection. If you don't, you are not protected against viruses that have been released into the computer world since you bought the product.

Installing Norton AntiVirus for Windows NT

When you install Norton AntiVirus exactly as directed by the on-screen instructions, you will have complete virus protection as soon as the installation is completed. This includes:

- Norton AntiVirus loaded automatically each time you start your computer.
- An automatic scan of your hard disks once per week to ensure they stay virus-free.
- Protection when you download files from the Internet.

Installation requirements

You need administrator-level privileges to install Norton AntiVirus for Windows NT. You don't need administrator-level privileges to run Norton AntiVirus after installation.

The minimum computer requirements are:

- 16 MB of memory (32 MB or more recommended)
- Microsoft Windows NT version 4.0
- 16 MB of free hard disk space

Installing

For the most complete protection, click Next on all the setup panels to accept the preset options.

To start install for Windows NT:

- 1 To install from a CD, do one of the following:
 - Insert the CD into the CD-ROM drive. After a moment, the Norton AntiVirus setup program starts automatically.

If the Norton AntiVirus setup program does not start automatically, Autorun may be disabled on your computer. To manually start Norton AntiVirus setup from a CD:
 - Insert the Norton AntiVirus CD in your CD-ROM drive, double-click the My Computer icon on the Windows desktop, double-click your CD-ROM drive, then locate and double-click Setup.



To install from floppy disks:

- Insert Norton AntiVirus Disk 1 in the A: drive, click Start on the Windows taskbar, click Run, type **A:SETUP** in the text box, then click OK.
- 2 Follow the on-screen instructions. *Questions?* See [page 11](#).

Questions when installing

Norton AntiVirus helps you install by giving you on-screen directions and highlighting the recommended actions. You make the following choices:

What the choices are	What you should do	Why?
Select the folder for Norton AntiVirus.	Accept the preset choice.	There's no reason not to. The choice is there for unusual circumstances.
Schedule weekly scans of your hard disks that run automatically?	Leave this checked.	A weekly scan makes sure your disks stay virus-free.
Automatically start Auto-Protect.	Leave this checked.	Auto-Protect constantly monitors your computer to make sure a virus doesn't infect.
Norton AntiVirus has detected a Netscape browser. Do you want to install plug-ins?	Choose Yes.	Lets Norton AntiVirus scan files for viruses when you download using a Netscape browser.
Run LiveUpdate after installation.	Leave this checked if you have a modem or Internet connection.	LiveUpdate connects to a special Symantec site and updates Norton AntiVirus automatically to protect against newly discovered viruses.
Scan for viruses after installation.	Leave this checked.	Makes sure that your computer is virus-free.

Uninstalling Norton AntiVirus

To uninstall Norton AntiVirus:

- On the Windows taskbar, click Start, point to Programs, point to Norton AntiVirus, click Uninstall Norton AntiVirus.

About Norton AntiVirus

Norton AntiVirus for Windows NT is the most sophisticated and powerful product available to safeguard your computer from virus infection, no matter what the source. You are protected from viruses that spread from hard or floppy disks, viruses that travel across networks, and even viruses that are transmitted across the Internet.

Is my computer protected against viruses?

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. After the installation, Norton AntiVirus automatic protection features continually safeguard your computer while you work. If a virus is found, Norton AntiVirus guides you through the process of eliminating it.

The Norton AntiVirus preset options balance efficiency with maximum protection; you do not need to change anything. Once you install Norton AntiVirus, you are immediately protected from computer viruses.

Here's what Norton AntiVirus does automatically:

- Checks programs for viruses at the time you use them.
- Scans your computer for viruses once per week.
- Checks floppy disks for boot viruses when you use them.
- Logs all viruses found.

Here's what you can do with Norton AntiVirus:

- Scan specific files, folders, or entire drives for viruses.
- Schedule virus scans to run at predetermined times.

- Update virus definitions files regularly.
- Submit potentially infected files to the Symantec AntiVirus Research Center for analysis.

What is a computer virus?

A computer virus is, simply, a computer program written by an ill-intentioned programmer. A virus program is designed in such a way that, when run, it attaches a copy of itself to another computer program. Thereafter, whenever the infected program is run, the attached virus program activates and attaches itself to other programs. For example, a computer virus, which your computer may get by running an infected program from a borrowed floppy disk, infects other programs on your computer. A computer virus, like a biological virus, lives to replicate.

In addition to replicating, some computer viruses are programmed specifically to damage data by corrupting programs, deleting files, or even reformatting your entire hard disk. Many viruses, however, are not designed to do serious damage; they simply replicate or display messages.

Viruses can only infect files and corrupt data. They do not infect or damage hardware, such as keyboards or monitors. Though you may experience strange behaviors such as screen distortion or characters not appearing when typed, a virus has, in fact, merely affected the programs that control the display or keyboard. Your disks themselves are not physically damaged, just the data stored on them.

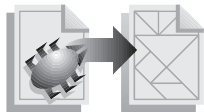
Virus infection cycle

There are three stages in the life of computer viruses: infection, detection, and recovery. In the infection stage, a virus infects a file in your computer. In the detection stage, the virus is identified and isolated. In the recovery stage, the virus is eliminated. Unless the virus is eliminated, it continues to infect other files and possibly damage data on your disks. Table 1-1, "Details of the virus life cycle," details each stage.

Norton AntiVirus is the most effective tool available to break this virus infection cycle. With Norton AntiVirus and its automatic protection features, you can prevent viruses from ever infecting your computer in the first place.

Table 1-1 Details of the virus life cycle

Infection



Source

Reused floppy disks from unknown sources
Disks from home or school
Disks borrowed from friends
Programs downloaded from BBSs or the Internet
Software from non-reputable dealers
Re-shrink-wrapped or opened software
Pirated software
Preformatted floppy disks

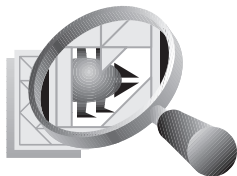
Infection

Boot from infected disk
Reboot with infected floppy disk left in drive
Run infected program or open infected document

Spread

Share disk or infected program or document
Log on to network
Email with infected programs or documents

Detection



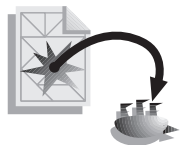
Observation

Strange system behavior
Files missing or programs not working

Utility

Virus detected by antivirus software

Recovery



Cleanup

Reinstall programs from master disks
Repair files with antivirus software
Restore from uninfected backup

Followup

Rescan all files to find source of infection
Scan all floppy disks to find source of infection
Discard backups that may be infected
Increase virus protection for a while

Prevention



Use Norton AntiVirus to prevent virus infection

How Norton AntiVirus protects you

A known virus is one that 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 disks and files for viruses, it is searching for these telltale virus signatures. If an item 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 files. For this reason, you should update your virus definitions files regularly so that Norton AntiVirus has the information it needs to find all known viruses. For instructions on getting the latest virus definitions files, see [Chapter 4, “Keeping up with new viruses,”](#) on page 49.

The Norton AntiVirus scanner is the heart of Norton AntiVirus protection. It searches for virus signatures when you initiate manual scans, schedule scans to run at specific times, and by the Auto-Protect feature every time a file is used.

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. For information on how to scan files, folders, or drives, see [“Scanning for viruses”](#) on page 25.

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. For information on scheduling scans, see [“Scheduling virus scans”](#) on page 29.

Auto-Protect

Auto-Protect, the Norton AntiVirus automatic protection feature, scans program files, documents, document template files, and spreadsheets for viruses whenever they are used. Auto-Protect is already turned on after

installation, unless you specifically turn it off. For information on customizing Auto-Protect, see [“Customizing automatic protection”](#) on page 71.

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 virus information to provide maximum protection. 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 regularly 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. For information on how to receive the latest definitions, see [“Automatically updating virus definitions”](#) on page 49.

Quarantine

Sometimes Norton AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions. Or, you have a file you think is infected that is not being detected. The Norton AntiVirus Quarantine safely isolates virus-infected files on your computer. A virus in a Quarantined item cannot spread.

From the Quarantine, a file can be sent over the Internet directly to the Symantec AntiVirus Research Center (SARC) for analysis. See [“Using the Quarantine”](#) on page 77 for information.

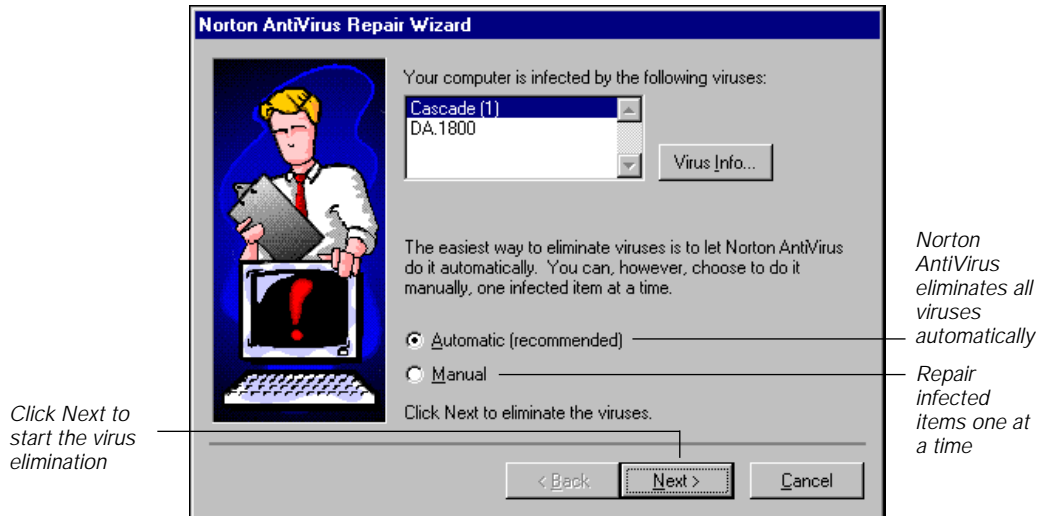
How Norton AntiVirus warns you

Norton AntiVirus warns you of possible virus infection in different ways, depending upon when the virus was detected:

- During manual or scheduled scans (see Figure 1-1)
- By Auto-Protect (see Figure 1-2)

If a virus is detected during a manual or scheduled scan, the Norton AntiVirus Repair Wizard (Figure 1-1) appears so you can eliminate the virus automatically. For instructions on using the Repair Wizard, see [“Eliminating viruses detected during scans”](#) on page 39.

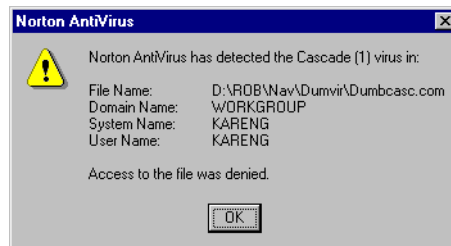
Figure 1-1 Norton AntiVirus Repair Wizard



Norton AntiVirus Auto-Protect, which constantly monitors for viruses, immediately displays an alert whenever an event concerning viruses occurs. Figure 1-2 shows an example of an Auto-Protect alert. The action taken for an infected item depends on your Auto-Protect configuration.

For instructions to configure Auto-Protect alert responses, see [“Customizing automatic protection”](#) on page 71.

Figure 1-2 Windows NT Auto-Protect alert



Virus risk under Windows NT

Computer viruses are classified by their targets, which are the items they infect:

- Boot viruses: Some viruses can infect disks by attaching themselves to special programs in areas of your disks called boot records and master boot records. These areas contain the programs your computer uses to start up.
- Program viruses: These viruses infect executable files, such as word processing, spreadsheet, computer game, or operating system programs.
- Macro viruses: In many word processing and spreadsheet applications, you can record a macro that stores a series of actions. Later, you can run the macro and automatically repeat the same actions. Macro viruses infect data files with macro capabilities. For example, Microsoft Word document and template files and Microsoft Excel spreadsheets are susceptible to macro virus attacks.

Boot viruses

Boot viruses are a particular risk under Windows NT. When a computer starts up, it runs the boot record (or bootstrap) program and reads other information from the boot records to ready itself for work. A boot virus activates at system startup, before the Windows NT operating system is loaded. In essence, boot viruses are operating system independent.

All hard and floppy disks have boot records, whether or not they also contain operating system files. A disk does not have to be bootable to be infected by a boot virus; data disks can contain boot viruses too. A typical way a computer gets a boot infection is to restart with an infected floppy disk inadvertently left in the drive. Even if the floppy disk is not a boot disk, the virus will activate and spread.

Windows NT manages memory differently than MS-DOS. If Windows NT can load despite a boot virus infection, the virus is disabled in memory. Your computer is still infected, but the virus does not show its usual symptoms or spread while Windows NT is running. Even if Windows NT boots normally, your computer is at risk each time you start up. The virus may activate during the boot and damage data on the drive. Many times, however, you won't be able to start up at all. If you boot into MS-DOS on a

multi-boot system, the virus is not disabled. All disks, including floppies, are at risk.

Program viruses

Windows NT inherits all MS-DOS program viruses, which do infect Windows NT executables, but does not yet have Windows NT-specific viruses.

Under Windows NT, DOS programs are run in DOS memory space. While in memory, an infected DOS program can continue to infect other programs and interfere with normal operations. Generally, program viruses remain active in your computer's memory after an infected program is executed until you end the DOS session.

If you have multiple DOS sessions open simultaneously, memory for all of them can be infected. Closing one does not remove the virus from memory for all of them. If a program virus is detected during a scan, close all DOS sessions and scan again.

Note: Norton AntiVirus also scans Microsoft Word documents and Excel spreadsheets when scanning program files. Although these are not program files, they can be infected by a new class of viruses called "Macro viruses."

Macro viruses

Modern applications include powerful macro systems. You can write entire macro-programs that run within the word processor or spreadsheet environment and are attached directly onto word processing and spreadsheet files. The ability to attach one or more macros to a data file is a powerful feature, however, this ability also makes it possible to create macro viruses.

When an infected document or spreadsheet is loaded, the application also loads any accompanying macros that are attached to the file. If one or more of the macros meet certain criteria, the application will also immediately execute these macros. Macro viruses rely upon this auto-execution capability to gain control of the application's macro system. Once the macro virus has been loaded and executed, it attaches its virus macro programs onto other documents. If this new file is later opened on

another computer, the virus will once again load, be launched by the application, and find other files to infect.

For macro viruses, the application serves as the operating system. A single macro virus can spread to any of the platforms on which the application is installed and running. For example, a single macro virus that infects in Microsoft Word could conceivably spread to Windows 3.x, Windows 95, Window NT, and the Macintosh.

Security considerations

Because of its flexibility, Windows NT presents special problems for virus control. Under the NT file system (NTFS), you can set different access permissions to the file, folder, or object (such as the boot records) level for each user or group. Not all users will be able to scan all items.

For example, a Windows NT-based computer may be used in any of the following ways:

- Standalone, single-user computer
- Networked, single-user computer
- Shared computer with multiple password logons
- Server

A scan of boot records requires administrator-level rights in any configuration. For standalone computers, the logged-on user generally has administrator-level rights. For other configurations, it becomes the administrator's responsibility.

For shared computers, file access is often limited to one's own files. Users must be vigilant to protect their files, and one user must be designated administrator to protect the system files and boot records.

In any network, the risk of infection is greatly magnified, since a virus can spread rapidly. For servers, an administrator must initiate scans. Note that you can scan files on any drive to which you are connected.

The following tables list the required access privileges when using Norton AntiVirus. If an access denied dialog box is displayed, first make sure that you have the necessary boot record, folder, or file permissions for the operation.

Table 1-2 Boot record access privileges

Permissions	Scan/Detect	Repair	Delete
Administrator-level privileges	Yes	Yes	Yes

Table 1-3 Folder access privileges

Folder (+File) Permissions	Scan/Detect	Repair	Delete
Full Control	Yes	Yes	Yes
Change (RWXD) (RWXD)	Yes	Yes	Yes
Add and Read (RWX) (RX)	Yes	No	No
Read (RX) (RX)	Yes	No	No
Add (WX) (not specified)	No	No	No
List (RX) (not specified)	No	No	No
No Access	No	No	No

Table 1-4 File access privileges

File Permissions	Scan/Detect	Repair	Delete
Full Control (RWD)	Yes	Yes	Yes
Modify (RW)	Yes	Yes	No
Read (R)	Yes	No	No

MS-DOS and Windows NT

Many computers are configured to permit booting into either Windows NT or MS-DOS. As you might expect, virus exposure increases greatly. For example, viruses that cannot infect because Windows NT restricts access to boot records, have free reign under MS-DOS. Further, a boot virus infection from a DOS session may prevent Windows NT from loading.

Using Norton AntiVirus

A virus can become active only if you start (or attempt to start) your computer from a disk infected with a boot virus, if you run an infected program, or open an infected document, template, or spreadsheet. As soon as you install Norton AntiVirus, your computer is protected from computer viruses.

Tips to avoid viruses

Some precautions you can take to minimize your virus risk:

- Make sure automatic protection is turned on at all times. Automatic protection is already set up for you when you install Norton AntiVirus using the preset options. For more information, see [“Customizing automatic protection”](#) on page 71.
- Perform a manual scan (or schedule a scan to occur automatically) of your hard disks once per week. These scans supplement automatic protection and confirm that your computer is virus-free. A scan is already scheduled to run automatically once per week when you install Norton AntiVirus using the preset options. See [“Scanning for viruses”](#) on page 25 and [“Scheduling virus scans”](#) on page 29.
- Scan all floppy disks before first use. For directions, see [“Scanning for viruses”](#) on page 25.
- Update your virus definitions files regularly. For directions, see [“Automatically updating virus definitions”](#) on page 49.
- Make periodic backups of your hard disk.
- Buy legal copies of all software you use and make write-protected backups.

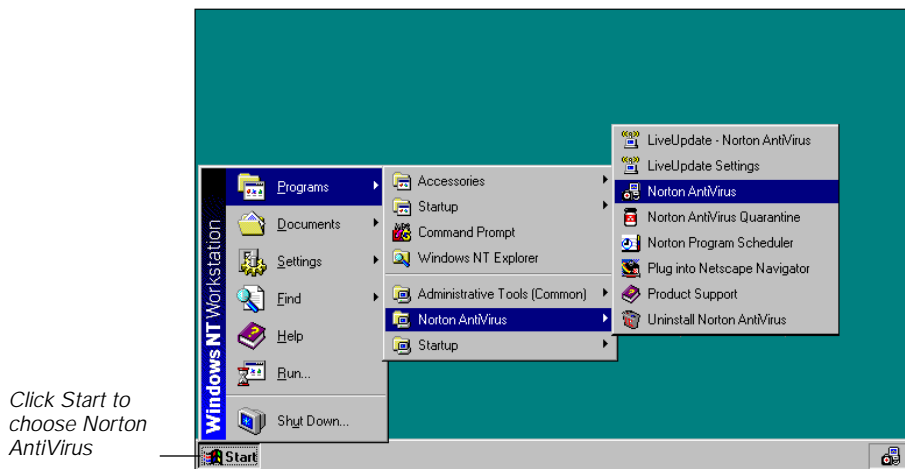
Starting and exiting Norton AntiVirus

You use the Norton AntiVirus main window to initiate scans for viruses, schedule scans that run automatically, view or change configuration options, or update virus definitions files. If you installed Norton AntiVirus using the preset options, Auto-Protect is always running. For information about Auto-Protect, see [“Enabling and disabling Auto-Protect”](#) on page 32.

To start Norton AntiVirus:

- Click Start on the Windows taskbar, point to Programs, point to Norton AntiVirus, and click Norton AntiVirus (Figure 2-1). The Norton AntiVirus for Windows main window appears (see Figure 2-2).

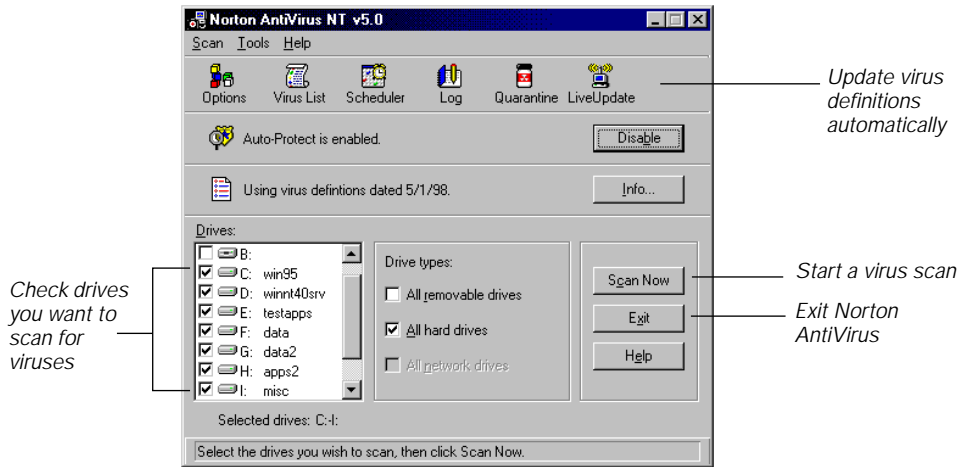
Figure 2-1 Starting Norton AntiVirus



To exit Norton AntiVirus:

- Click Exit in the Norton AntiVirus main window.

Figure 2-2 The Norton AntiVirus main window



Getting help

The Norton AntiVirus help system has step-by-step procedures to keep your computer safe from viruses.

To get help using Norton AntiVirus:

Do one of the following:

- Right-click any option in a Norton AntiVirus screen and choose What's This for a brief definition of the option.
- Choose Contents from the Help menu.
- Click the Help button on any Norton AntiVirus screen.

Scanning for viruses

You can initiate a virus scan at any time. As a general practice, scan your hard disks at least once a week or schedule a scan to occur automatically. Always scan floppy disks before you use them for the first time and always scan files downloaded from bulletin boards and other online services.

At the end of each scan, Norton AntiVirus reports its findings. If any problems are found, the Norton AntiVirus Repair Wizard appears so you can direct repairs (see ["Eliminating viruses detected during scans"](#) on page 39). After the problems are dealt with, as well as after a scan with no

problems found, a scan summary details everything that happened during the scan.

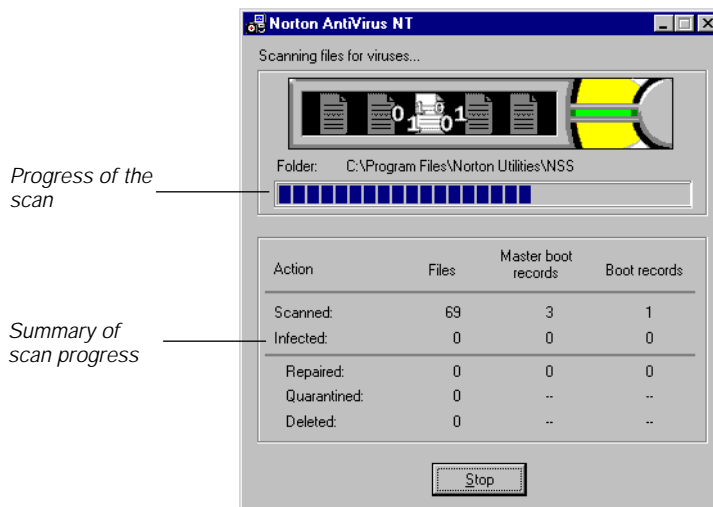
Tip: The Norton AntiVirus preset options balance maximum protection with efficiency during scans. In most cases you do not need to change anything. You can, however, customize what is scanned and what to do if a virus is found. For directions, see “[Customizing manual scan options](#)” on page 57.

To scan one or more drives:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window, check specific drives to scan in the Drives list box or select multiple drives by checking items in the Drive Types group (see Figure 2-2).
- 3 Click Scan Now.

The Scan dialog box reports the progress of the scan.

Figure 2-3 Scan in progress



To scan an individual file:

- 1 In the Norton AntiVirus main window, select File from the Scan menu.
- 2 Select the file you want to scan.

- 3 Click Open.

To scan an individual folder:

- 1 In the Norton AntiVirus main window, select Folders from the Scan menu.
- 2 Select the folder you want to scan.
- 3 Click Scan.

To scan a specified path:

- 1 In the Norton AntiVirus main window, select Path from the Scan menu.
- 2 Enter the path to scan.
You can enter a UNC path as well (for example, \\Central\Apps).
- 3 Click Scan.

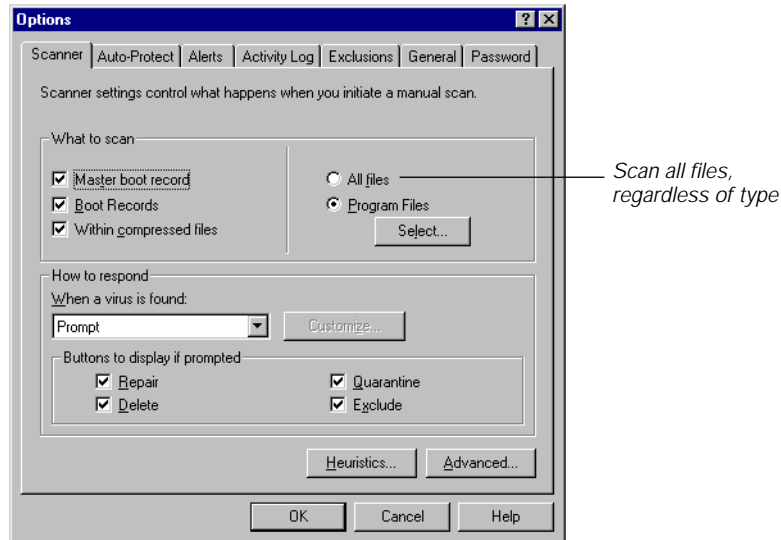
Norton AntiVirus is preset to scan only program files, documents, document templates, and spreadsheets during a scan, because these are the only types of files from which viruses spread. Occasionally, such as after a virus attack, scan all files to make sure files that don't appear as regular program files get scanned as well.

To scan all files, regardless of type:

- 1 In the Norton AntiVirus main window, click Options.
- 2 Click the Scanner tab (Figure 2-4).
- 3 Select the All Files option.
- 4 Click OK to return to the Norton AntiVirus main window.
- 5 Select the drives to scan and click Scan Now.

For more information about selecting Program Files or All Files for scanning, see [“Selecting which files to scan”](#) on page 62.

Figure 2-4 Scanner options tab

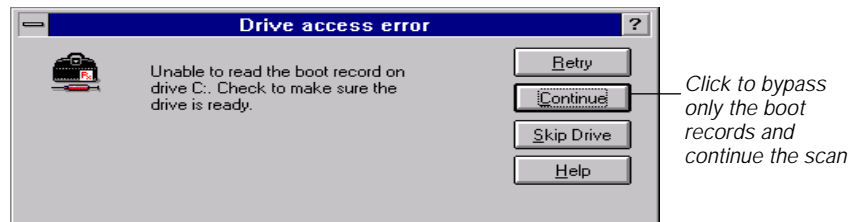


Bypassing boot record scans

Norton AntiVirus is preset to scan your disk's boot records for viruses as part of its regular operation. Boot records are special areas of your disks that contain programs and other information your computer uses to start up.

As a security precaution, some Windows NT systems are configured to prevent users from accessing these disk areas. You must have administrator-level privileges to scan boot records. If you see a dialog box saying that you cannot access the boot records (Figure 2-5), you can set a configuration option to bypass boot record scans.

Figure 2-5 Access to boot records denied



To bypass boot record scans:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Scanner tab.
- 3 Uncheck the first two items in the What To Scan group box:
 - Master Boot Record
 - Boot Records
- 4 Click OK to save your settings and close the dialog box.

Caution: Unchecking these options to disable hard disk boot record scans also disables floppy disk boot record scans.

For detailed instructions to set other scanner options, See [“Customizing manual scan options”](#) on page 57.

Scheduling virus scans

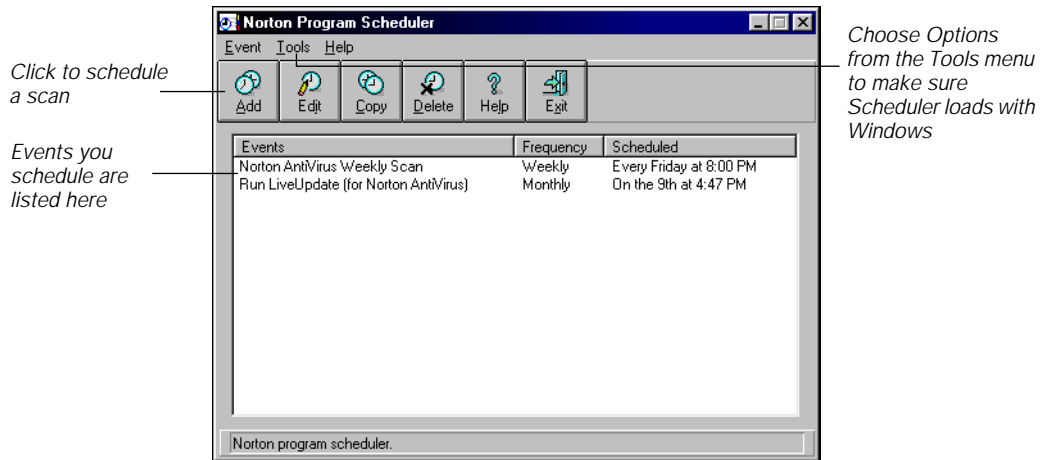
You can schedule a weekly virus scan that runs unattended. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working. You can schedule virus scans that run unattended on either specific dates and times or at periodic intervals. A scan is already scheduled to run automatically once per week when you install Norton AntiVirus using the preset options.

To access the Scheduler, use one of the following methods:

- Click Scheduler in the Norton AntiVirus main window.
- Choose Norton Program Scheduler from the Windows Start menu.

If no events are already scheduled, the Edit, Copy, and Delete buttons are dimmed.

Figure 2-6 The Norton Program Scheduler

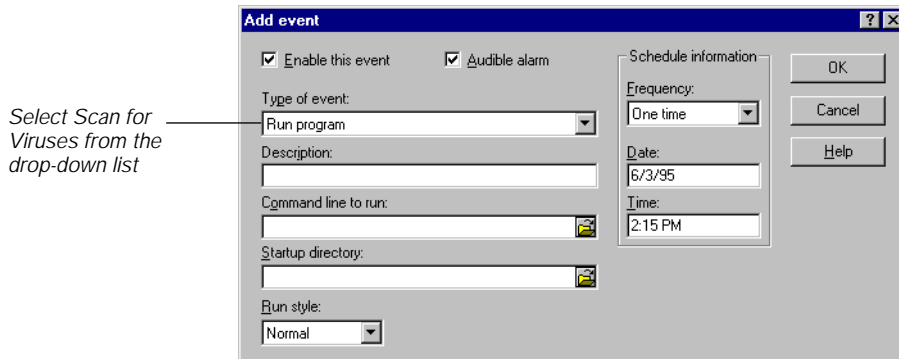


To schedule virus scans:

- 1 Click Add.

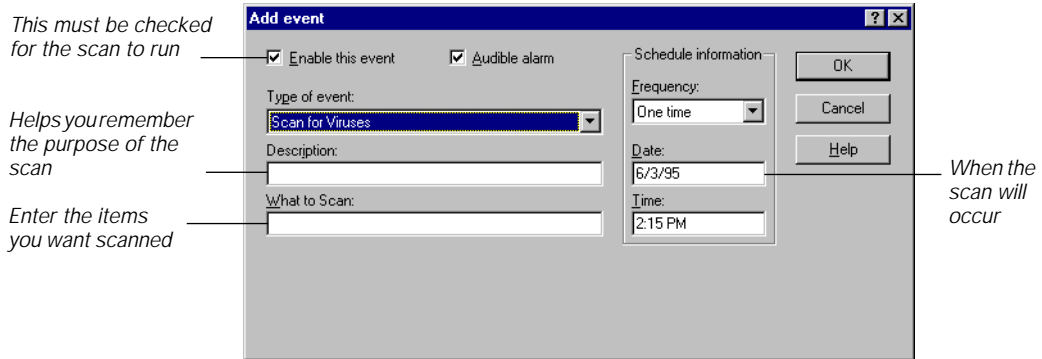
The Add Event dialog box appears so you can schedule any type of event.

Figure 2-7 Add event dialog box



- 2 Select Scan For Viruses in the Type Of Event drop-down list.
The dialog box changes to accept information specific to a virus scan.

Figure 2-8 Add event dialog box with Scan for Viruses selected



3 Check Enable This Event.

If you uncheck this option, the scan won't run.

4 Check Audible Alarm to hear a beep when the scan starts.

5 Type a brief description in the Description text box.

This text will appear in the events list in the Scheduler dialog box.

6 Type the drive letter or pathname for the drive, folder, or file you want scanned in the What To Scan text box.

Note: Do not leave the What To Scan text box blank. You must specify what to scan.

To specify your hard disk, type the drive letter followed by a colon.

C:

To specify more than one item to scan, use a space between items.

C: D:\Applications

If the path uses spaces, enclose the item in double quotes.

"C:\Rad Was Here\Hithere.exe"

You can use any of the NAVW32.EXE switches with Scheduler. For a list of command-line switches, see Appendix C, "Using command-line switches," on page 95.

7 Select how often you want the scan to occur in the Frequency drop-down list.

8 Finish scheduling the scan by entering the correct time, day, or date information, if necessary.

- 9 Click OK. If prompted for confirmation, also click OK in the confirmation dialog box.

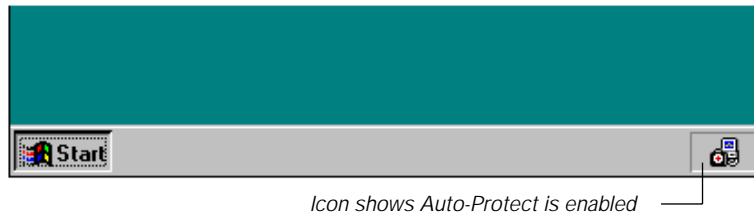
Tip: From a Windows NT command prompt, you can use the AT command to schedule multiple scans under Windows NT. For instructions on running the scanner (NAVWNT) directly from the command line, see Appendix C, “Using command-line switches,” on page 95.

Enabling and disabling Auto-Protect

Norton AntiVirus is preset to load Auto-Protect—the automatic virus protection technology—whenever you start your computer. The Norton AntiVirus Auto-Protect icon appears on the Windows taskbar (Figure 2-9).

Generally, you should not disable Auto-Protect. It is your best protection against viruses. There are, however, a few situations when you might want to disable Auto-Protect. For example, you are sometimes told to disable your antivirus software when you are installing new computer programs. In this case, disable Auto-Protect temporarily and then turn it back on again.

Figure 2-9 The Windows taskbar



To turn off Norton AntiVirus Auto-Protect temporarily:

Do one of the following:

- Right-click the Norton AntiVirus icon in the lower-right corner of the taskbar on your Windows desktop, then click Disable Auto-Protect.
- Double-click the Norton AntiVirus icon in the lower-right corner of the taskbar on your Windows desktop to open the Norton AntiVirus main window, then click Disable.



To turn on Norton AntiVirus Auto-Protect:

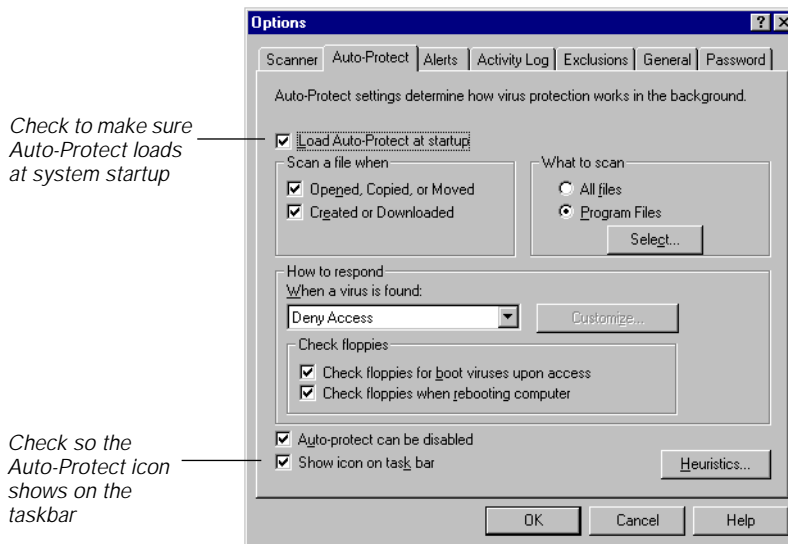
Do one of the following:

- Right-click the Norton AntiVirus icon in the lower-right corner of the taskbar on your Windows desktop, then click Enable Auto-Protect.
- Double-click the Norton AntiVirus icon in the lower-right corner of the taskbar on your Windows desktop to open the Norton AntiVirus main window, then click Enable.

To load Auto-Protect every time you start your computer:

- 1 Start Norton AntiVirus.
- 2 Click Options in the Norton AntiVirus main window (see Figure 2-2).
- 3 Click the Auto-Protect tab (Figure 2-10).

Figure 2-10 Setting Auto-Protect options



- 4 Check Load Auto-Protect At Startup.
- 5 Click OK.

Norton AntiVirus enables Auto-Protect immediately and every time your computer starts up thereafter.

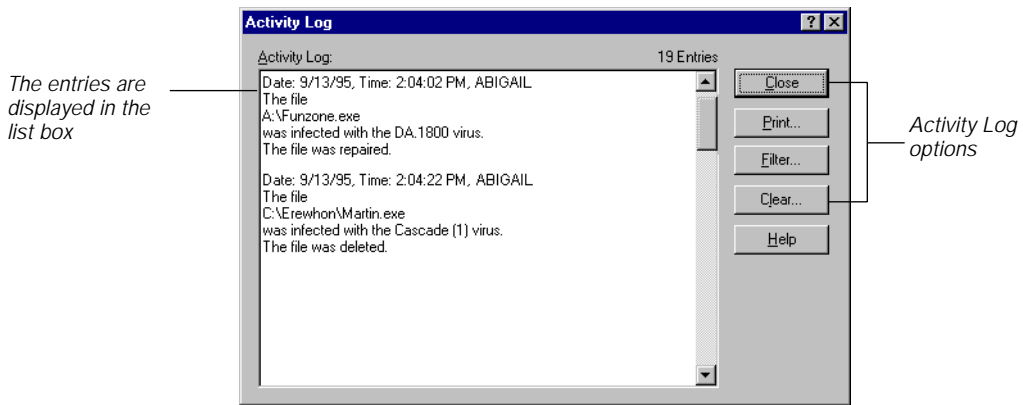
Viewing the Activity Log

The Activity Log file contains details of Norton AntiVirus activities, such as when problems were found and how they were resolved. For information on specifying what is stored in the Activity Log, see “Customizing the Activity Log” on page 69.

To view all entries in the Activity Log:

- 1 Click Log in the Norton AntiVirus main window.

Figure 2-11 The Activity Log



- 2 Click Close to exit the Activity Log.

Note: All Norton AntiVirus events are also logged in the Windows NT Application Event Log.

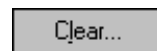
From the Activity Log dialog box you can also:



Click Print to print the Activity Log to a printer or a file. Only the entries currently displayed in the list box are printed. If you filter the Activity Log, only the filtered entries are printed.



Click Filter to limit the display to specific types of events, such as virus detections.

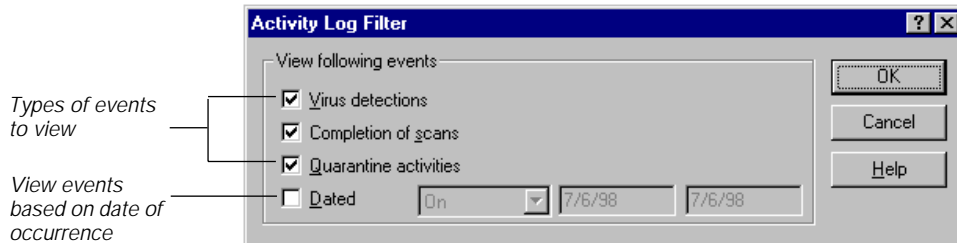


Click Clear to delete all of the entries in the Activity Log.

To filter the Activity Log entries:

- 1 Click Filter in the Activity Log dialog box (see Figure 2-11).

Figure 2-12 The Activity Log Filter



- 2 Check the types of events you want listed. If no entries match your filter, a No Items To Display dialog box appears instead. In this case, the filter changes are ignored and the previous settings are restored.
 - Virus Detections: Displays information on viruses.
 - Completion Of Scans: Displays information about when scans occurred. This option applies to manual and scheduled scans only.
 - Quarantine Activities: Displays information files sent to the Quarantine.
 - Dated: Indicates the date or range of dates for displaying the selected events. Select an option in the Dated drop-down list, then enter the date or dates to define the scope.
- 3 Click OK.

Internet protection

As part of regular operation, Norton AntiVirus for Windows NT with its default settings gives complete protection from Internet-borne viruses. No separate programs or Norton AntiVirus options changes are necessary. Auto-Protect scans program and document files automatically as they are downloaded, and files within compressed files when they are extracted (Options Auto-Protect tab, Scan A File When Created Or Downloaded option).

Netscape and Norton AntiVirus

For an additional level of protection, Norton AntiVirus detects whether Netscape is already installed during setup. If so, Norton AntiVirus asks whether to install itself as a Netscape helper application so that downloaded files are scanned for viruses automatically. If you install Netscape after Norton AntiVirus is installed, run the program NSPlugIn.exe in your Norton AntiVirus folder (by default, C:\Program Files\Norton AntiVirus).

Other Internet Browsers and Norton AntiVirus

If you choose not to use Auto-Protect, you can configure other browsers to use Norton AntiVirus as a helper application as well. To configure Internet browsers to use Norton AntiVirus, use the following command line as the application to launch for each MIME type and set of extensions:

```
"C:\Program Files\NAVNT\NAVWNT" /DOWNLOAD
```

Don't forget to include the double quotes ("). If you've installed Norton AntiVirus in a different folder, change the command line to the proper location.

The following table lists the standard MIME types and associated extensions.

Table 2-1

MIME type	Extensions
application/octet-stream	386, BIN, CLA, COM, CPL, DLL, DRV, EXE, NCP, NED, NNL, OCX, OVL, SCR, SYS, VBX, VXD
application/binary	386, BIN, CLA, COM, CPL, DLL, DRV, EXE, NCP, NED, NNL, OCX, OVL, SCR, SYS, VBX, VXD
application/zip	ZIP, LHA, LZH
application/msword	DOC, DOT
application/word	DOC, DOT
application/msexcel	XLB, XLM, XLS, XLT, XLW
application/x-excel	XLB, XLM, XLS, XLT, XLW

For more information about helper applications and MIME types, consult your Internet browser documentation or help system.

Eliminating viruses

Norton AntiVirus warns you of possible virus infection in different ways, depending upon when the virus was detected:

- During manual or scheduled scans: The Norton AntiVirus Repair Wizard appears at the end of the scan to eliminate all viruses found automatically. For more information, see “[Eliminating viruses detected during scans](#)” on page 39.
- By Auto-Protect: Auto-Protect, which is constantly monitoring your computer for viruses, displays a Virus Alert immediately when it detects an infected item. Auto-Protect uses a preconfigured response to deal with the virus. For more information, see “[Eliminating viruses detected by Auto-Protect](#)” on page 43.

Eliminating viruses detected during scans

The action Norton AntiVirus takes for an infected item detected during a scan depends on your scanner configuration. The options are Prompt, Notify Only, or one of several automatic responses. For directions to change settings, see “[Customizing manual scan options](#)” on page 57.

The default response is to Prompt. If the Scanner is set to Prompt and viruses are detected during a scan, the Norton AntiVirus Repair Wizard appears at the end of the scan (Figure 3-1). You can let Norton AntiVirus eliminate all viruses automatically or you can choose to eliminate the viruses manually, one item at a time.

If you specify another automatic response, the selected action takes place without interaction. The Scan Summary dialog box that appears at the end of the scan details all actions that were taken during the scan.

Figure 3-1 Norton AntiVirus Repair Wizard



To eliminate all viruses automatically:

- 1 Scan a drive, folder, or file with Norton AntiVirus.

The Repair Wizard appears only if a virus is detected (Figure 3-1).

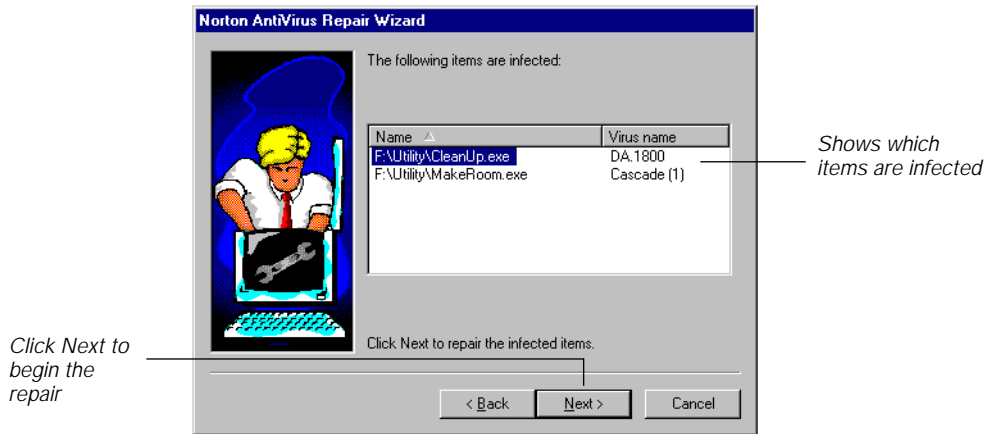
- 2 Select Automatic in the Norton AntiVirus Repair Wizard and click Next.

If you select Manual, see [“To resolve virus issues manually, item by item:”](#) on page 41 for directions.

- 3 Read each succeeding panel (Figure 3-2) to understand what Norton AntiVirus is doing, then click Next to continue.

The Repair wizard will not take any action without asking permission first.

Figure 3-2 Which items are infected



Tip: When the Repair Wizard finishes, the last panel summarizes what actions Norton AntiVirus performed. On this panel you can click More Info if you want details about the operations, or want to print a report about what was infected and repaired.

If you select Manual in the Norton AntiVirus Repair Wizard, the Problems Found dialog box (Figure 3-3) appears listing all infected items.

To resolve virus issues manually, item by item:

- 1 Select Manual in the Norton AntiVirus Repair Wizard (see Figure 3-1) and click Next.

The Problems Found dialog box (Figure 3-3) appears and lists each infected item.

- 2 Highlight an entry in the list box.

Details of the entry appear below, describing the type of problem that was found.

- 3 Read the message at the bottom of the dialog box to understand the type of problem that was found. It relates to the highlighted entry.
- 4 For information on the command buttons in the Problems Found dialog box, see **“Command buttons”** on page 42 then click the appropriate button.

Figure 3-3 Problems Found dialog box





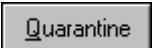


Command buttons

Table 3-1, “Command buttons,” explains all buttons that Norton AntiVirus may display in the Problems Found dialog box to respond to virus issues. Note that some buttons may be dimmed or not displayed at all for the following reasons:

- The option is not permitted for your particular Norton AntiVirus configuration. These options are set on the Scanner and Auto-Protect tabs. For information on setting options, see [Chapter 5, “Customizing Norton AntiVirus,”](#) on page 57.
- Norton AntiVirus has determined that a particular action cannot be performed in the current situation.

Table 3-1 Command buttons

Button	Result	Additional Information
	Eliminates the virus and returns the infected file or boot record to its original state.	See “ Eliminating viruses detected by Auto-Protect ” on page 43.
	Eliminates the virus by deleting the infected file.	Deleted files cannot be recovered. After the file is deleted, you must replace it yourself with an uninfected copy. Make sure the backup copy is not infected as well.
	Stops the current operation. If a scan is in progress, the scan stops.	Selecting Stop does not solve the problem reported. If it is a virus, the virus is prevented from activating, but remains on your computer and is still a source of risk.
	Continues the operation and excludes the file from notifications of this kind in the future.	Use this command button only when you are sure it isn't a real problem. Excluding a file means Norton AntiVirus won't warn you again. See “ Managing exclusions ” on page 65.
	Isolates the virus-infected file, but does not remove the virus.	Choose Quarantine if you suspect the infection is caused by an unknown virus and you want to submit the virus to the Symantec AntiVirus Research Center for analysis. See “ Submitting a file to SARC for analysis ” on page 79.

Eliminating viruses detected by Auto-Protect

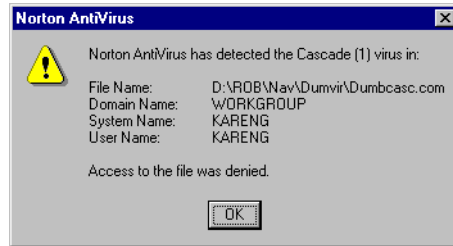
Norton AntiVirus Auto-Protect, which constantly monitors for viruses, immediately displays an alert whenever an event concerning viruses occurs (Figure 3-4). You are warned when a virus is found in any of the following situations:

- You are trying to run an infected program.
- You are trying to open an infected document or spreadsheet.

- You are trying to use a floppy disk infected with a boot virus.

The action Norton AntiVirus takes when it detects an infected item depends on your Auto-Protect configuration. The default response is to Deny Access. For directions to change Auto-Protect settings, see “[Customizing automatic protection](#)” on page 71.

Figure 3-4 A virus found alert



If Auto-Protect discovers a virus and is configured to deny access to the item, be sure to scan your disks to find and eliminate the virus and make sure it hasn't spread. There are three ways to treat a virus on your computer:

- Repair the infected item.
- Quarantine the infected item. If the virus can't be removed, you update your virus definitions and scan again. If the virus still can't be removed, submit the infected file to Symantec for analysis. See “[Submitting a file to SARC for analysis](#)” on page 79.
- Delete the infected file from the disk.

You cannot, however, delete infected system files, boot records, or master boot records because they contain information your computer uses to start up. For instructions on how to proceed if a repair cannot be made and the file cannot be deleted, see “[What to do if repair is unsuccessful](#)” on page 45.

Once you are certain that your system is virus-free, replace any files you deleted with uninfected copies. Make sure you scan the replacement files before copying them to your hard disk. If you forget which file needs replacing, look at the Activity Log for the name of the file. For information, see “[Viewing the Activity Log](#)” on page 34.

What to do if repair is unsuccessful

In the rare instance when Norton AntiVirus is unable to repair a file or boot record, you are notified that the repair was not successful.

Tip: Before you try anything else, make sure you have the latest virus definitions files and scan again. For instructions to get current files, see [“Automatically updating virus definitions”](#) on page 49.

Unable to repair a file

If Norton AntiVirus could not repair the infected file, you can either delete the file or isolate it in the Quarantine. From the Quarantine, a file can be sent over the Internet directly to the Symantec AntiVirus Research Center (SARC) for analysis. See [“Using the Quarantine”](#) on page 77 for directions.

If you choose to let Norton AntiVirus delete the infected file, you can replace it with an uninfected copy. Use an uninfected backup copy or the original program disk that came with the application. If you don't have a backup and can't find the original disks, try contacting the program's manufacturer for a replacement.

Unable to repair a system file

If the infected file is a system file, you cannot delete it. Restart your computer from the Windows NT Emergency Repair Disk that you created when you installed Windows to replace the file. If this fails, you will have to reinstall Windows NT.

Unable to repair a boot record

If Norton AntiVirus could not successfully repair the master boot record or a boot record on your hard disk, restart your computer from the Windows NT Emergency Repair Disk that you created when you installed Windows to attempt a repair. If this fails, you will have to reinstall Windows NT.

If Norton AntiVirus could not successfully repair a boot record on a floppy disk, you can still copy important files from the floppy disk to another disk. But be careful—the floppy disk is still infected. Scan any files you copy from the floppy disk for viruses again. After you've copied any important

files from the infected floppy disk, either discard the disk or reformat it (on an uninfected computer).

Removing viruses from compressed files

Although Norton AntiVirus will detect an infected file in a compressed file, it cannot repair the file in its compressed state. You must decompress the file first to eliminate the virus.

To remove viruses from infected compressed files:

- 1 Create a temporary folder.
- 2 Click the Auto-Protect icon in the Windows taskbar or double-click the minimized Auto-Protect icon on the desktop to disable Auto-Protect temporarily.
- 3 Decompress the compressed file into the temporary folder.
- 4 Delete the infected compressed file.
- 5 Scan the temporary folder and repair or delete any infected files.
- 6 Recompress the files in the temporary folder, if desired.
- 7 Click the Auto-Protect icon in the Windows taskbar or double-click the minimized Auto-Protect icon on the desktop to enable Auto-Protect.

Note: If the compressed file is in the Quarantine, see [“Treating compressed files in the Quarantine”](#) on page 80.

Dealing with common problems

This section explains how to resolve some common problems that may arise while you are using Norton AntiVirus.

After scanning and removing a virus, it continues to infect files

Cause: The source of the infection is a floppy disk.

Solution: Scan all floppy disks. For directions, see [“Scanning for viruses”](#) on page 25.

Cause: The virus may be contained in an executable file with a non-standard file extension.

Solution: Modify the Scanner options to scan All files instead of Program files. Scan all disks that you use and repair all infected files. Add any infected files' extensions to the Program File Extensions list.

For information on how to change the selection of files for scanning, see [“Selecting which files to scan”](#) on page 62 and [“Specifying program file extensions”](#) on page 63.

Cause: The virus is active in another open DOS session.

Solution: Close all open DOS sessions and scan again.

A program does not work properly after repair

Cause: Although Norton AntiVirus removes the virus, the virus may have damaged the file beyond complete repair.

Solution: Replace the program with an uninfected original.

Keeping up with new viruses

Norton AntiVirus uses the information in its virus definitions files to detect viruses during scans. As new viruses are discovered, their virus definitions are added to the virus definitions files. To prevent newly discovered viruses from invading your computer, update your virus definitions files regularly.

Automatically updating virus definitions

To ensure that you always have current virus protection, Norton AntiVirus can update the virus definitions files on your computer automatically. All that is required on your part is one of the following:

- An Internet connection
- A properly connected modem

Make it a practice to update your virus definitions at least monthly.

Figure 4-1 Update virus definitions automatically



To update virus definitions automatically:

- 1 In the Norton AntiVirus main window, click LiveUpdate.
- 2 In the How Do You Want To Connect drop-down list, select one of the following:
 - Find Device Automatically: Norton AntiVirus determines if you have an Internet connection or must connect using your modem.
 - FTP: 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.
- 3 Click Next to start the automatic update.

Whichever method you choose, Norton AntiVirus makes the connection, downloads the proper files, and installs them on your computer. You don't have to do anything else.

When the update is finished, read the new Text Documents (*.TXT) in your Norton AntiVirus folder that are downloaded also. They contain late-breaking information about newly discovered viruses and any special precautions that you should take.

Note: If the connection is made by modem, a long distance toll charge may appear on your telephone bill.

Using LiveUpdate Email

Whenever a major virus threat is discovered that requires an update to your virus protection, Symantec can notify you by email so you can run LiveUpdate immediately. The email includes an attachment that can start a LiveUpdate session for you.

To receive LiveUpdate Email:

- 1 Point your Internet browser to www.symantec.com/avcenter/newsletter.html
- 2 Fill out the registration form.
- 3 Click the Subscribe Me button.

Symantec will notify you by email whenever protection updates are available.

To start a LiveUpdate session from the LiveUpdate Email:

- When you receive a LiveUpdate Email, launch or run the email attachment called LIVEUPDT.NLU from your mail program.
You must launch or run the attachment; simply reading or viewing it will not work.

When the attachment runs, it automatically starts a LiveUpdate session on your computer. You don't have to do anything else.

Scheduling an automatic LiveUpdate

After you successfully complete a LiveUpdate to verify operation, you can schedule future LiveUpdates to run unattended at a predetermined frequency and time. For more information about using the Norton Program Scheduler, see [“Scheduling virus scans”](#) on page 29.

To schedule an automatic LiveUpdate:

- 1 Do one of the following to access the Norton Program Scheduler:
 - Click Scheduler in the Norton AntiVirus main window.
 - Choose Norton Program Scheduler from the Windows Start menu.

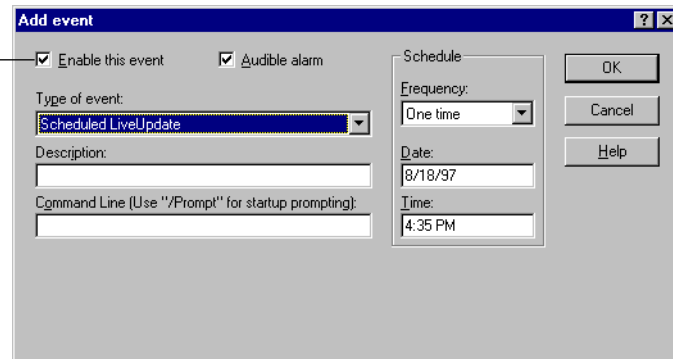
- 2 Click Add.

The Add Event dialog box appears.

- 3 Select Scheduled LiveUpdate in the Type Of Event drop-down list.
The dialog box changes to accept information specific to LiveUpdate.

Figure 4-2 Add event dialog box with Scheduled LiveUpdate

This must be checked for the LiveUpdate to run



- 4 Check Enable This Event.
If you uncheck this option, the LiveUpdate won't run.
- 5 Check Audible Alarm to hear a beep when LiveUpdate starts.
- 6 Type a brief description in the Description text box.
This text will appear in the events list in the Scheduler dialog box.
- 7 Type /PROMPT in the Command Line text box if you want to okay the LiveUpdate session when it is scheduled to run.
- 8 Select how often you want the LiveUpdate to occur in the Frequency drop-down list.
- 9 Finish scheduling the LiveUpdate by entering the correct time, day, or date information, if necessary.
- 10 Click OK. If prompted for confirmation, also click OK in the confirmation dialog box.

Manually updating virus definitions

Symantec provides the latest virus definitions files with a program called Intelligent Updater, available for download at <http://www.symantec.com>

To install the new virus definitions:

- 1 Download the Intelligent Updater program to any folder on your computer.
- 2 From a My Computer or Windows NT Explorer window, double-click the Intelligent Updater program.
- 3 Follow all prompts displayed by the update program.

The update program installs the new virus definitions files in the proper folder automatically.

- 4 Initiate a scan with Norton AntiVirus to make sure any newly discovered viruses are detected.
- 5 Disable and re-enable Auto-Protect so that Auto-Protect uses the new virus definitions files as well.

Read the new Text Documents (*.TXT) in your Norton AntiVirus folder for late-breaking information about newly discovered viruses and any special precautions that you should take.

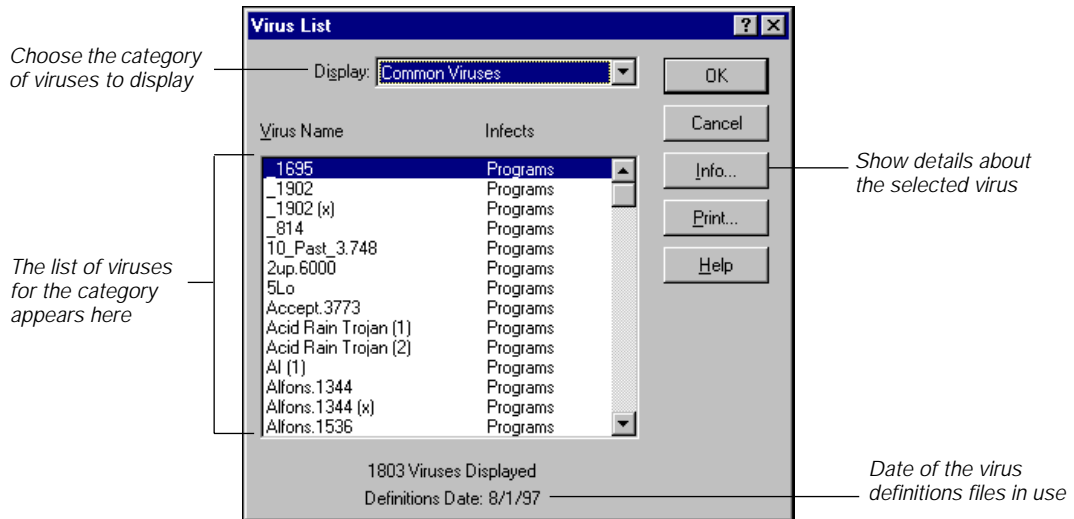
Viewing the Virus List

You can see which viruses Norton AntiVirus detects by viewing the list of virus names. These are the names of the viruses that can be identified from information in the virus definitions files. You can also view descriptions of particular viruses, including their symptoms and aliases.

To view the list of virus names:

- Click Virus List in the Norton AntiVirus main window.

Figure 4-3 The Virus List



The list box displays the name of the virus and what it infects. You can view different categories of viruses by selecting a category from the Display drop-down list box.

Table 4-1

All Viruses	Displays all of the viruses that Norton AntiVirus can detect.
Common Viruses	Displays the most common viruses. These are viruses that you are most likely to encounter.
Program Viruses	Displays viruses that can infect program files that you run.
Boot Viruses	Displays viruses that can infect boot records or master boot records on disks.
Stealth Viruses	Displays viruses that try to conceal themselves from attempts to detect or remove them.
Polymorphic Viruses	Displays viruses that appear differently in each infected file, making detection more difficult.
Multipartite Viruses	Displays viruses that infect both program files and boot records.

Table 4-1 (continued)

Macro Viruses	Displays viruses that infect documents, document templates, and spreadsheets.
Windows Viruses	Displays viruses that infect Windows programs.
Malicious Programs	Displays Trojan horse programs (programs that masquerade as something useful but actually destructive), including ActiveX and Java applets.

Info...

Click Info to view details about a particular virus, such as likelihood, characteristics, and aliases.

Print...

Click Print to print the virus list to a printer or to a file.

To search for a virus name:

- 1 Activate the virus list by clicking inside the Virus Name list box (see Figure 4-2).
- 2 Start typing the name of the virus you want to find.

A text box appears below the list box. As you type the consecutive letters in the virus name, the highlight moves to the corresponding virus name.

If the virus name you are looking for is not in the list, the list may not be displaying all viruses. To display all virus names, select All Viruses in the Display drop-down list box.

Customizing Norton AntiVirus

The preset options from your Norton AntiVirus installation provide excellent protection and significantly reduce your risk of virus infection. Most users only need to set alert options. You can, however, tailor all of Norton AntiVirus to suit your computing environment.

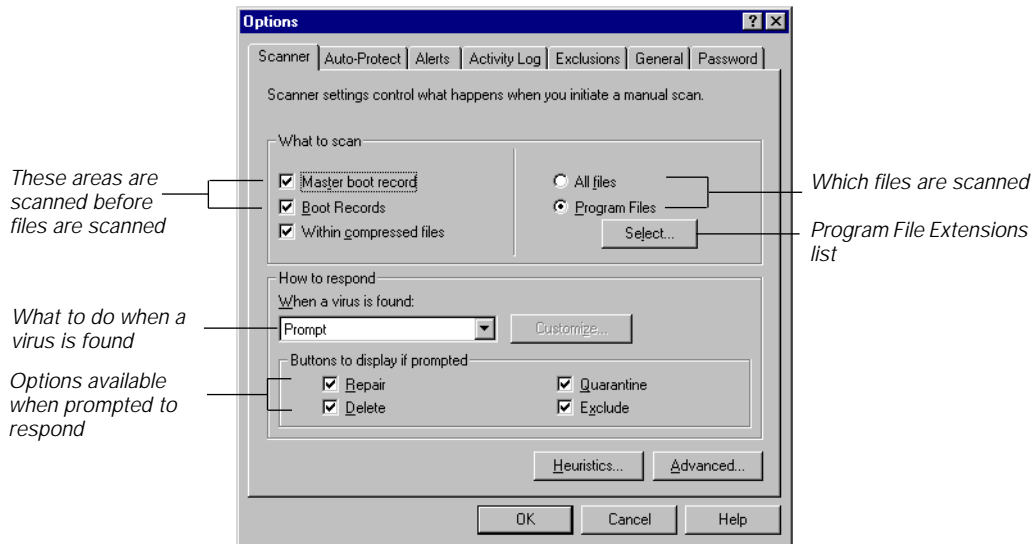
Customizing manual scan options

The manual scan options affect scans you initiate when you click the Scan Now button in the Norton AntiVirus main window or when scheduled scans occur. You specify what is scanned and how to respond if a virus is detected.

To customize what to scan:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Scanner tab.

Figure 5-1 Scanner Settings



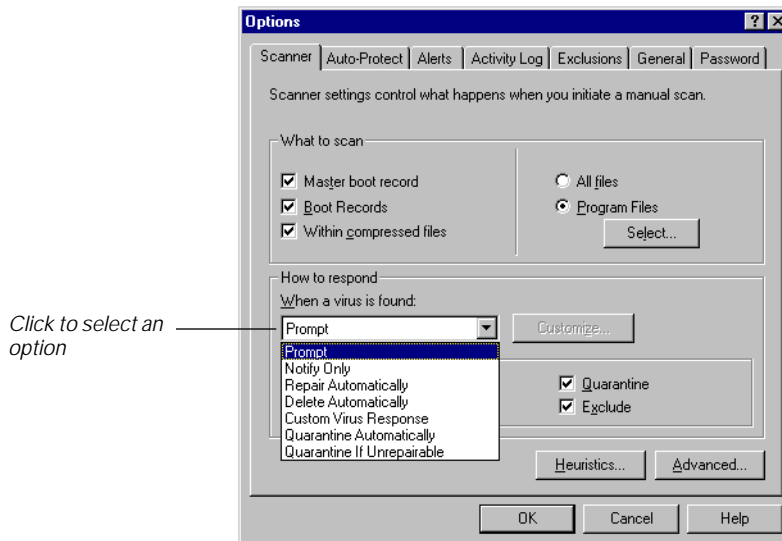
- 3 In the What To Scan group box, select which areas of your computer Norton AntiVirus should scan before it scans files. By default, these options are checked for general safety.
 - Master Boot Record: Checks for viruses in the master boot record on your hard disk.
 - Boot Records: Checks for viruses in the boot records on your hard disk and on any floppy disks you scan.
 - Within Compressed Files: Norton AntiVirus scans files compressed using popular compression utilities. Compressed files within compressed files are not scanned. Scanning time may increase slightly if you have many compressed files.
- 4 Also, in the What To Scan group box, specify the types of files to scan:
 - All Files: Scans all files in the specified folder or drive, including files less susceptible to viruses.
 - Program Files: Scans files that are most likely to become infected. Only the files with an extension that is specified in the Program File Extensions list are scanned. For more information on which option to choose and on the Program File Extensions list, see [“Selecting which files to scan”](#) on page 62.

- 5 Click OK to save your settings and close the dialog box, or continue with the next procedure.

To customize how to respond when a virus is found:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Scanner tab (see Figure 5-1).
- 3 Select an option in the How To Respond drop-down list box.

Figure 5-2 What to do when a virus is found



- **Prompt:** Informs you when a virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.
- **Notify Only:** Informs you when a virus is detected. You will not be able to repair, delete, or quarantine the infected file.
- **Repair Automatically:** Repairs an infected file or boot record without asking you. The results of the repair are displayed at the end of the scan and are also recorded in the Activity Log.

Norton AntiVirus is preset to make backup copies of files before they are repaired. For more information, see “[Setting backup options](#)” on page 70.

- **Delete Automatically:** Deletes an infected file without asking you. The file deletion results are displayed at the end of the

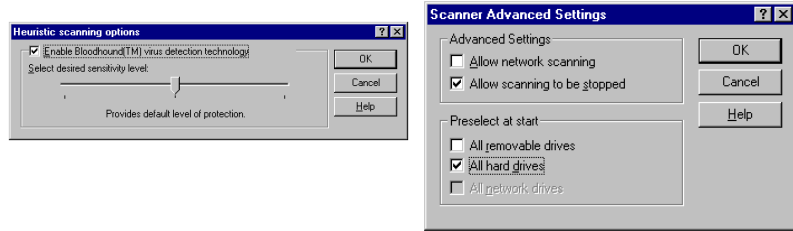
scan and are also recorded in the Activity Log. Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be recovered by any means.

- Custom Response: Lets you specify different actions for file, macro, and boot virus detections. After selecting Custom Response, click Customize to specify the actions.
 - Quarantine Automatically: Isolates the virus-infected file in a special safe location for later treatment. You can submit the file to the Symantec AntiVirus Research Center (SARC) for analysis or download newer virus definitions and scan again. For information, see [“Submitting a file to SARC for analysis”](#) on page 79.
 - Quarantine If Unrepairable: Attempts a repair of an infected file automatically. If the repair is not successful, the virus-infected file is isolated in the Quarantine. For information, see [“Submitting a file to SARC for analysis”](#) on page 79.
- 4 If you selected Prompt in step 3, specify in the Buttons To Display If Prompted group box which options you want Norton AntiVirus to make available when a virus is found:
- Repair: Lets you repair the file or boot record. If the virus infects an item that cannot be repaired, such as a file that is in use, the button will be dimmed.
 - Delete: Lets you delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button will be dimmed.
 - Quarantine: Lets you continue scanning without resolving the problem. The the virus-infected file is isolated in a special safe location for later treatment. For information, see [“Submitting a file to SARC for analysis”](#) on page 79.
 - Exclude: Lets you exclude the file from future checks for known viruses. Use caution when using this button; it can reduce your protection against viruses.
- 5 Click OK to save your settings and close the dialog box, or continue with the next procedure.

To set additional scanning options:

- 1 Click the Heuristics button in the Scanner tab (see Figure 5-2). The Heuristic Scanning Options dialog appears (Figure 5-3).

Figure 5-3 Additional Scanner Settings



- 2 Make sure that Enable Bloodhound Virus Detection Technology is checked.

Norton AntiVirus includes a new technology called Bloodhound that detects a high percentage of new and unknown viruses to dramatically increase your virus protection against difficult to detect viruses.
- 3 You can drag the pointer to increase Bloodhound processing in a high-risk environment, but scanning will take a bit longer.
- 4 Click Ok to close the Heuristic Scanning Options dialog.
- 5 Check the Advanced Settings options that you want to enable:
 - Allow Network Scanning: Lets you scan network drives. For network scanning restrictions, see the next section, “Scanning network drives.”
 - Allow Scanning To Be Stopped: Lets you halt a scan in progress. When this option is checked, the Stop button is available during a scan.
- 6 Specify in the Preselect At Start group box the drives that you want automatically selected in the Drives list box when you start Norton AntiVirus.
- 7 Click OK to save your settings and close the dialog box.

Scanning network drives

Because you do not always have the same access privileges to a network drive as you have to a local drive, there are some restrictions when scanning network drives with Norton AntiVirus.

Drive access privileges	Operations you can perform
None	None
Read-Only	Scan, but not repair, delete, or quarantine infected files
Read-Write	Scan, repair, delete, and quarantine

Scanning network drives is more time consuming than scanning local drives. Other users may be creating, deleting, or moving files on a drive while Norton AntiVirus is scanning.

Selecting which files to scan

In most situations, scanning program files is adequate because viruses only infect and spread from these types of files. Following is an explanation of the file type options, so you can decide which setting is best for your situation.

All files

The All Files option scans every file—data files (such as databases, text files, and spreadsheets) and program files (such as system files, word processing programs, and utility programs). Scanning all files takes longer but includes any executable files, Microsoft Word documents, or Microsoft Excel spreadsheets that have non-standard file extensions. Scanning for program files only is usually sufficient unless a virus is found on your computer. In this case, scan all files to ensure that every file on your disk is virus-free.

Program files only

The Program Files option scans files with extensions contained in the Program File Extensions list. The list contains the most common extensions for executable files, which are most likely to become infected and spread viruses. Scanning only program files is sufficient in most cases.

Note: The extensions for Microsoft Word documents and Excel spreadsheets are included in the program files group. Although these are not program files, they can be infected by the class of viruses called macro viruses.

If you are using a specialized program that has an executable file extension not on the Program File Extensions list, you can add it to the list. Even if you don't add the extension to the list, Norton AntiVirus will probably catch the virus during a scan. A virus is most likely to infect one or more files that are on the Program File Extensions list before it infects a program with a non-standard file extension. After the virus is found, you can scan all files to ensure that every file on your disk is virus-free. For information on setting these options, see [“Customizing manual scan options”](#) on page 57 and [“Customizing automatic protection”](#) on page 71.

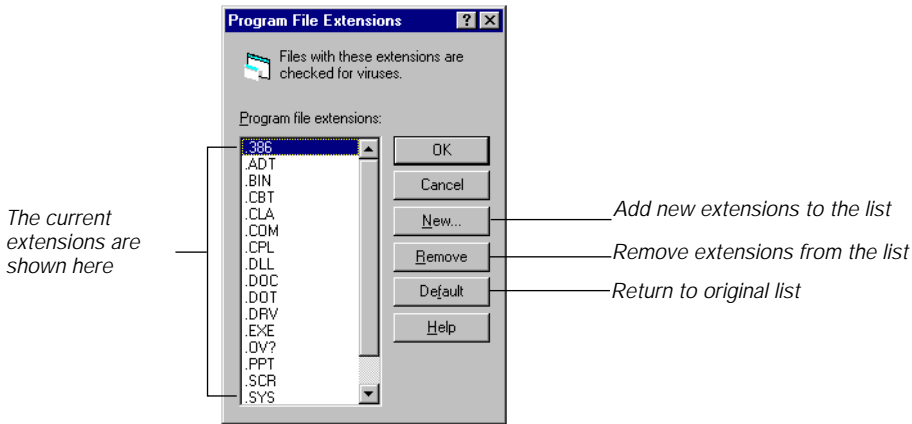
Specifying program file extensions

Norton AntiVirus uses the Program File Extensions list when scanning. The list contains the file extensions for files most likely to become infected and spread viruses. File extensions are always three characters.

To view the current program file extensions:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Scanner tab.
- 3 Select the Program Files option in the What To Scan group box (see Figure 5-1).
- 4 Click Select.

Figure 5-4 Program File Extensions dialog box

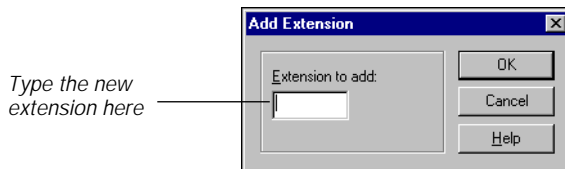


The Program File Extensions list contains the majority of program file extensions. If you use custom applications that use unique file extensions, add them to the list.

To add a program file extension:

- 1 Click New in the Program File Extensions dialog box (see Figure 5-4).

Figure 5-5 New Program File Extension dialog box



- 2 Type the new file extension in the Extension To Add text box.
You can use wildcards in the extension, but not to represent all three characters. For example, .OV? represents files with extensions that begin with .OV, such as .OVL and .OV1.
- 3 Click OK.

To remove a program file extension:

- 1 Select the file extension in the Program File Extensions dialog box (see Figure 5-4).
- 2 Click Remove.
- 3 Click OK.

To reset the list of program file extensions:

- 1 Click Default in the Program File Extensions dialog box (see Figure 5-4).
The list of extensions returns to the way it was when you installed Norton AntiVirus.
- 2 Click OK.

Managing exclusions

Norton AntiVirus uses the Exclusions List in all scans. No entries in the list are scanned for viruses. You assign exclusions to *items*—drives, folders, groups of files, or single files. If you move or rename a file that is set up as an exclusion using its pathname, you automatically invalidate it.

Although you can add items to the Exclusions List manually, it is not a good idea unless you are sure of what you are doing. Typically, you might assign exclusions to network volumes or tree branches that you don't want scanned as part of regular operation.

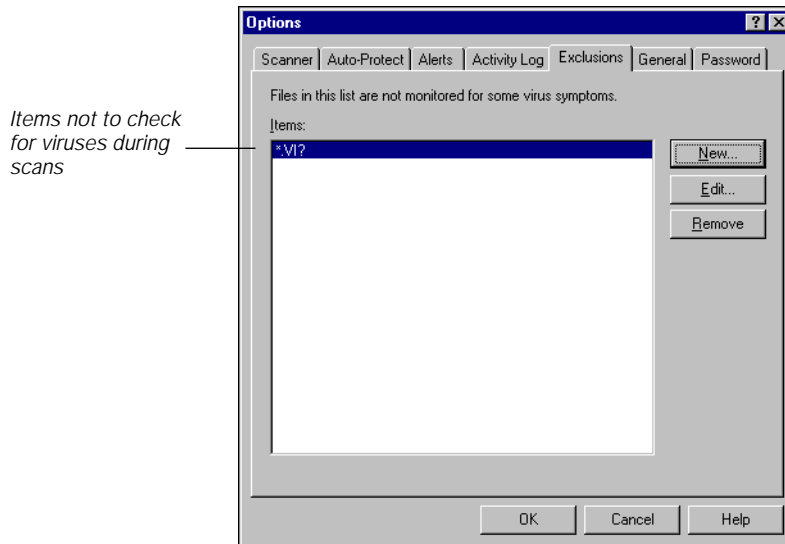
In practice, items are added to the Exclusions List when you click the Exclude button in the Problems Found dialog box at the end of a scan. If you exclude an item from a scan, a virus can creep in.

Caution: Unless you have a specific reason for excluding something from a scan, don't modify the default list.

To view the Exclusions List:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Exclusions tab.

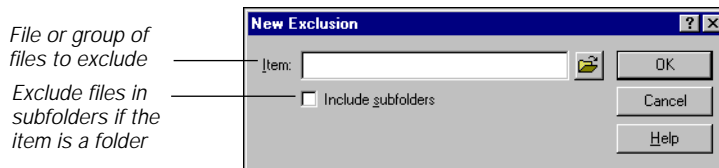
Figure 5-6 Exclusions List Settings tab



To manually add exclusions:

- 1 Click New in the Exclusions tab (see Figure 5-6).

Figure 5-7 New Exclusion dialog box



- 2 Type the pathname for the file or group of files in the Item text box.
- 3 Check Include Subfolders if you want files in descending folders of the item to be excluded also.
- 4 Click OK.

To remove an exclusion:

- 1 Select a file or group of files from the Items list box in the Exclusions tab (see Figure 5-6).
- 2 Click Remove.

The exclusion is removed from the list so that complete virus protection is restored.

- 3 Click OK.

To modify an existing exclusion:

- 1 Select a file or group of files from the Items list box in the Exclusions tab (see Figure 5-6).
- 2 Click Edit and make the desired changes.
- 3 Click OK.

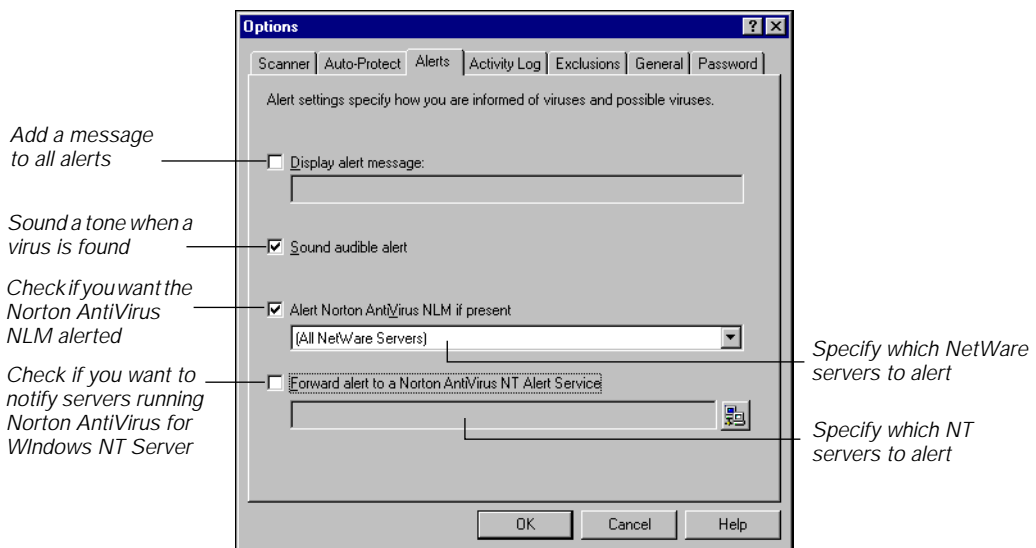
Customizing alerts

Alert settings define how Norton AntiVirus informs you or other users on the network that it has detected a virus. These options apply to all scans that Norton AntiVirus performs, including scans you initiate, scheduled scans, and scans performed automatically by Auto-Protect.

To customize alerts:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Alerts tab.

Figure 5-8 Alerts Settings



- 3 Check Display Alert Message to add a message with instructions or special warnings to all alerts that Norton AntiVirus displays, then enter the message in the text box.
- 4 Check Sound Audible Alert if you want Norton AntiVirus to sound a tone when it alerts you of a virus.
- 5 Check Remove Alert Dialog After to specify how long notification dialog boxes stay on your screen, then enter a number of seconds (between 1 and 99) in the Seconds text box.
- 6 Click OK.

Sending network alerts

When a virus or other Norton AntiVirus event is detected on a workstation, Norton AntiVirus can send alerts to the Norton AntiVirus for NetWare NLM over Novell NetWare networks. You can specify a particular server or notify all NetWare servers running the NLM. For networks with Windows NT servers, alerts can be forwarded to servers running Norton AntiVirus for Windows NT Server.

To set network alert options:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Alerts tab (see Figure 5-8).
- 3 For Novell NetWare networks, check the Alert Norton AntiVirus NLM If Present check box.
- 4 Do one of the following:
 - In the drop-down list box, select a specific NetWare server running the Norton AntiVirus NLM.
 - In the drop-down list box, select All NetWare Servers. Norton AntiVirus will alert all NetWare servers running the NLM.
- 5 For Windows NT servers, check Forward Alert To A Norton AntiVirus NT Alert Service.
- 6 Either type the name of the message relay target or click the browse button and select it from the network tree.
- 7 Click OK.

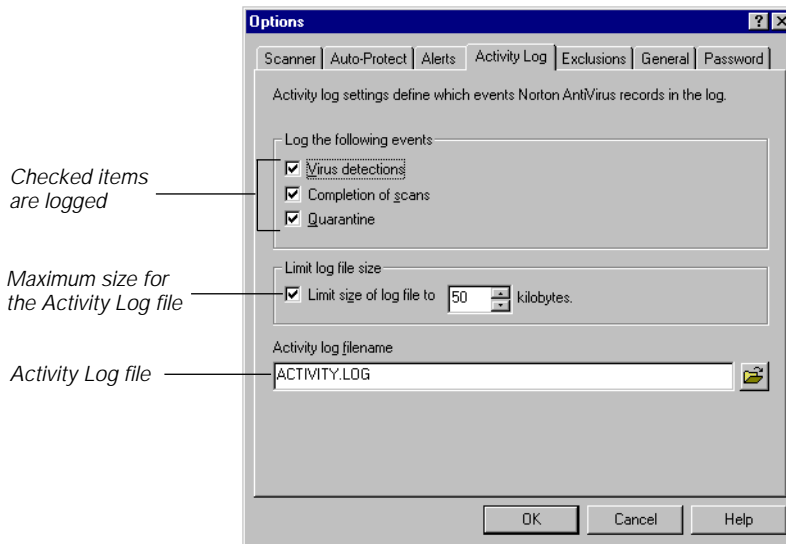
Customizing the Activity Log

The Activity Log contains a history of Norton AntiVirus activity. For example, Norton AntiVirus is preset to record detections of known viruses and what action was taken on infected files (whether they were repaired, deleted, quarantined, added to the Exclusions List, or left untouched).

To customize the Activity Log:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Activity Log tab.

Figure 5-9 Activity Log Settings tab



- 3 In the Log Following Events group box, check each type of event that you want Norton AntiVirus to record:
 - Known Virus Detections: Records detections of known viruses (viruses identified in the Virus List).
 - Completion Of Scans: Records the date and ending time of scans that you initiate and scheduled scans.
 - Quarantine: Records Quarantine activity.

- 4 If you want to limit the size of the Activity Log file, check Limit Size Of Log File To, then type the desired size in the Kilobytes text box.

When the specified file size is reached, each new entry added to the activity log replaces the oldest entry.

- 5 Type the pathname for the Activity Log file in the Activity Log Filename text box.
- 6 Click OK to save your settings and close the dialog box.

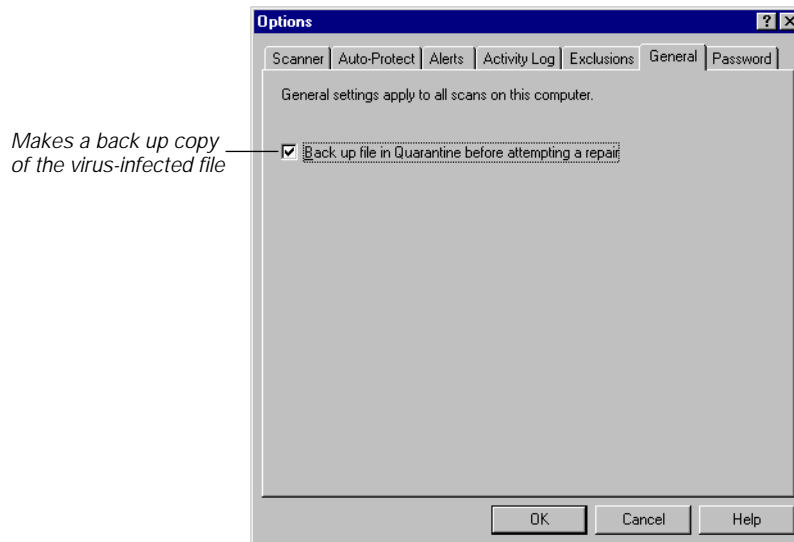
Setting backup options

As a safety precaution, Norton AntiVirus is preset to make a backup copy of a file before it attempts a virus repair. The files are stored in a section of the Quarantine called Backup Items. Delete the backup files after you determine that the repair operation is successful. Even though the infected backup files can't be run from the Quarantine, they contain viruses. For more information, see [“Using the Quarantine”](#) on page 77.

To change backup settings:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the General tab.

Figure 5-10 General Settings tab



- 3 Check Back Up File Before Attempting A Repair to have Norton AntiVirus make a copy of the infected file before repairing it.
- 4 Click OK.

Customizing automatic protection

The automatic protection feature protects your computer against viruses in the following ways:

- Checks programs for viruses when you run them.
- Checks floppy disks for viruses when you access them.
- Prevents viruses from getting onto your computer when you copy or install files on your system.

For information on other options that affect Auto-Protect scans, see [“Customizing manual scan options”](#) on page 57.

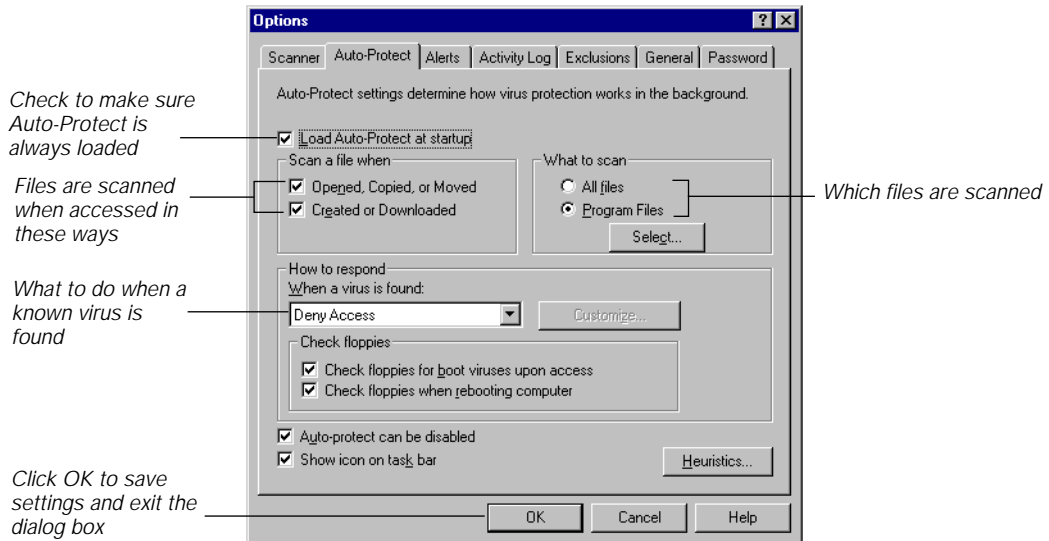
Auto-Protecting program files

Norton AntiVirus can check for viruses whenever you open a file or run a program. You specify what is scanned and how to respond if a virus is detected.

To Auto-Protect program files:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Auto-Protect tab.

Figure 5-11 Auto-Protect Settings



- 3 Check Load Auto-Protect At Startup to make sure automatic protection is on every time you start your computer. Unchecking this option significantly reduces protection against viruses.
- 4 Specify in the Scan A File When group box when Norton AntiVirus should scan the files you use:
 - Opened/Run: Scans files when they are opened. For example, when you copy a file, Norton AntiVirus scans the file you are copying and scans a program file each time you run it.
 - Created: Scans files when they are created on your drive by an installation program, by decompressing files, by downloading files from the Internet or a bulletin board system, or copying files from another computer.
- 5 Select an option in the What To Scan group box:
 - All Files: Scans all files that you access, including files less likely to contain viruses.
 - Program Files: Scans files that are most likely to become infected. Only the files with an extension in the Program File Extensions list are scanned.

For more information on which option to choose and on the Program File Extensions list, see [“Selecting which files to scan”](#) on page 62.

- 6 Click OK to save your settings and close the dialog box, or continue to the next procedure.

To customize how to respond when a virus is found:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Auto-Protect tab (see Figure 5-11).
- 3 Select an option for how to respond in the When A Virus Is Found drop-down list box:
 - Deny Access: Prevents you from using a file when a known virus is detected. These events are recorded in the Activity Log.
 - Prompt: Informs you when a virus is found and lets you choose how to respond. Select Prompt to have the most control over what happens to an infected file.
 - Repair Automatically: Repairs an infected file or boot record without notifying you. The results of the repair are recorded in the Activity Log. If the file cannot be repaired, access is denied. Norton AntiVirus is preset to make backup copies of files before they are repaired. For more information, see [“Setting backup options”](#) on page 70.
 - Delete Automatically: Deletes an infected file without asking you. The file deletion results are recorded in the Activity Log. Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be recovered.
 - Custom Response: Lets you specify different actions for file, macro, and boot virus detections. After selecting Custom Response, click Customize to specify the actions.
 - Quarantine Automatically: Isolates the virus-infected file in a special safe location for later treatment. You can submit the file to the Symantec AntiVirus Research Center (SARC) for analysis or download newer virus definitions and scan again. For more information, see [“Submitting a file to SARC for analysis”](#) on page 79.
 - Quarantine If Unrepairable: Attempts a repair of an infected file automatically. If the repair is not successful, the virus-infected file is isolated in the Quarantine. For more information, see [“Submitting a file to SARC for analysis”](#) on page 79.
- 4 Check Auto-Protect Can Be Disabled if you want to be able to temporarily turn automatic protection off by clicking the Auto-Protect icon on the Windows taskbar.

- 5 Check Show Icon On Taskbar to remind you that automatic protection is in force and to permit the temporary enabling or disabling of Auto-Protect.
- 6 Click OK to save your settings and close the dialog box or continue to the next procedure.

Auto-Protecting floppy disks

Because boot viruses are most likely to spread through floppy disks, it is important to check each floppy disk you use. Norton AntiVirus can monitor floppy disks when you work with them or if you accidentally leave one in your disk drive while shutting down your computer.

To Auto-Protect floppy disks:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Auto-Protect tab.
- 3 In the Check Floppies group box (see Figure 5-11), specify how you want Norton AntiVirus to check for boot viruses on floppy disks:
 - Check Floppies For Boot Viruses Upon Access: Checks for boot viruses on each floppy disk you access (such as, when you list the folder, copy a file, write to a file, or run a file).
 - Check Floppies When Rebooting Computer: Checks a floppy disk in drive A: for boot viruses when you shut down your computer. This protects you from boot viruses spreading from floppy disks inadvertently left in a drive.
- 4 Click OK to save your settings and close the dialog box.

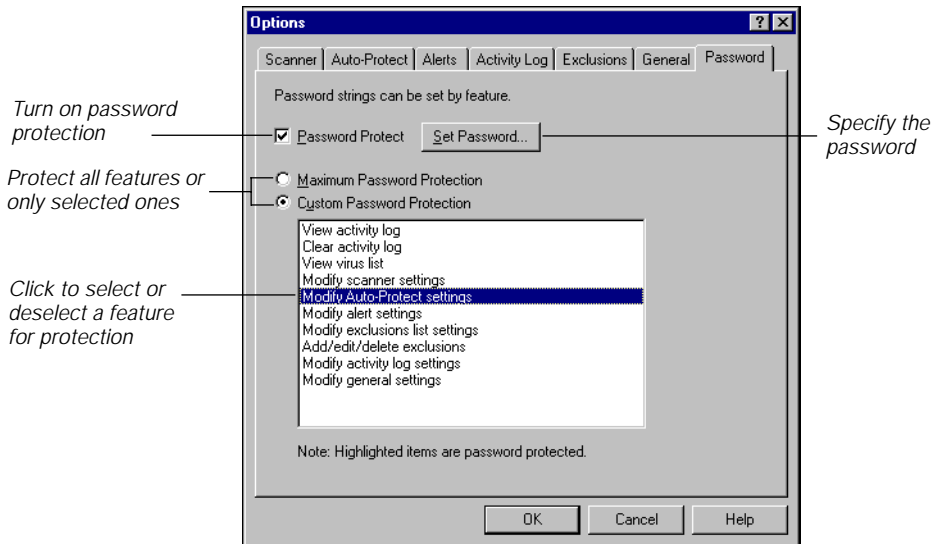
Setting password protection

Password protection guarantees that your Norton AntiVirus configuration will not be modified. You can select features to protect, or protect all features.

To password-protect features:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Password tab.

Figure 5-12 Password Settings



- 3 Check Password Protect to turn on the password protection feature.
- 4 Do one of the following:
 - To protect all Norton AntiVirus features, select Maximum Password Protection.
 - To protect only specified features, select Custom Password Protection, then click the features you want to protect in the list box.
- 5 Click Set Password and type the password you want to use in the Set Password dialog box. The same password applies to all protected options.

Passwords can be from 1 to 16 characters in length and are not case-sensitive (a is the same as A). As you type, Norton AntiVirus replaces the characters on the screen with asterisks (*) for security.

- 6 Click OK in the Set Password dialog box, then click OK.

Norton AntiVirus will also prompt for the password before allowing changes to the password protection options.

To change your password:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Password tab (see Figure 5-12).
- 3 Type your existing password in the Verify Password dialog box that appears.
- 4 Click Set Password.
- 5 Type your existing password in the Old Password text box.
- 6 Type the new password in the New Password text box.
- 7 Type it again in the Confirm New Password text box, then click OK.

To remove password protection:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Password tab (see Figure 5-12).
- 3 Type your existing password in the Verify Password dialog box that appears.
- 4 Do one of the following:
 - To remove password protection completely, uncheck Password Protect.
 - To remove password protection for some of the protected features, select Custom Password Protection and click items in the list box to deselect them.
- 5 Click OK.

Managing the Quarantine

Sometimes Norton AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions. Or, you have a file you think is infected that is not being detected. The Norton AntiVirus Quarantine safely isolates virus-infected files on your computer. A virus in a Quarantined item cannot spread.

From the Quarantine, a file can be sent over the Internet directly to the Symantec AntiVirus Research Center (SARC) for analysis. SARC will determine if your file is infected. If the file is not infected, SARC will report the results to you. If a new virus is discovered in your submission, SARC will create and send you special updated virus definitions to detect and eliminate the new virus on your computer.

You must have an Internet connection to submit a sample and an email address to receive a reply. You are notified by email with the results of the analysis within seven days.

Using the Quarantine

Files are quarantined in one of three ways:

- You select Quarantine after receiving a Norton AntiVirus alert.
- Norton AntiVirus is configured to Quarantine infected items rather than repair them or to Quarantine them if they cannot be repaired. For information about configuration options, see “[Customizing manual scan options](#)” on page 57 and “[Customizing automatic protection](#)” on page 71.
- You suspect a file is infected and manually add it to the Quarantine.

In addition to quarantined files, the Quarantine stores two other groups of items:

- **Backup Items:** For data safety, Norton AntiVirus is preset to make a backup copy of a file before attempting a repair. These backups are stored in the Quarantine. After the repaired file is verified, you can delete the infected backup from the Quarantine.
- **Items Submitted To SARC:** Files sent to SARC for analysis are isolated. After receiving the results of the analysis, you can determine what to do with the item.

To access the Quarantine:

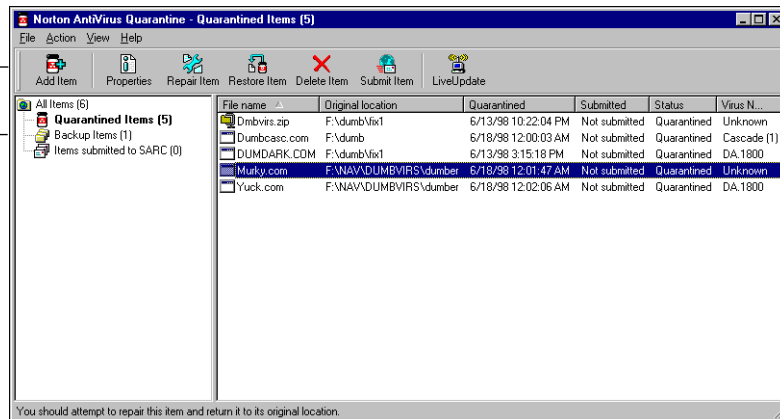
Do one of the following:

- In the Norton AntiVirus main window, click Quarantine.
- Click Start on the Windows taskbar, point to Programs, point to Norton AntiVirus, and click Norton AntiVirus Quarantine.

Figure 6-1 Norton AntiVirus Quarantine

*Actions you
can take from
the Quarantine*

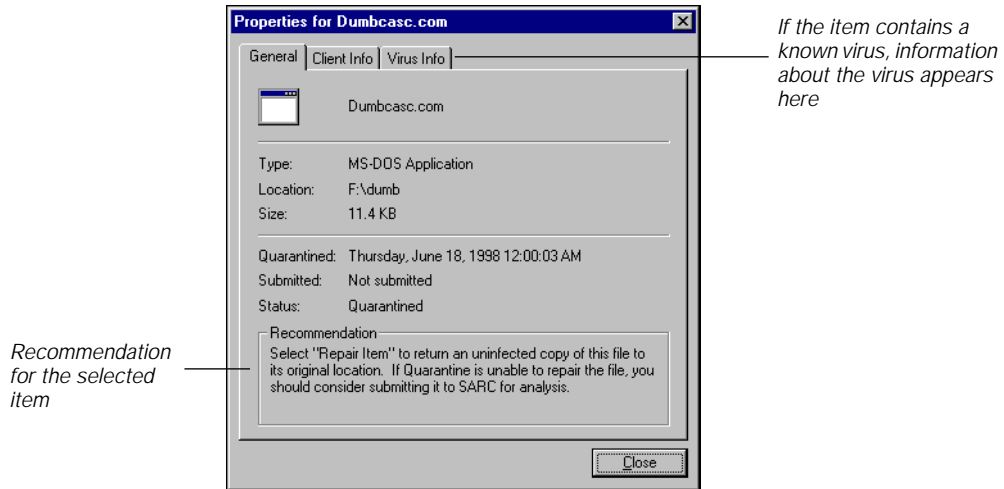
*Types of items
stored in the
Quarantine*



To get information about a quarantined item:

- 1 In the left panel, click Quarantined Items.
- 2 Do one of the following:
 - Select an item in the right panel and click Properties.
 - Double-click an item in the right panel.

Figure 6-2 Properties for quarantined item



Adding a file to the Quarantine manually

If you suspect that a file is infected but not being detected, you can isolate the file.

To manually add an item to the Quarantine:

- 1 Open the Quarantine.
- 2 Click Add Item.
- 3 In the Add To Quarantine dialog box, locate the file you want to add.

If the Remove File From Original Location option is checked, the potentially infected file can't be run accidentally.

- 4 Click Add.

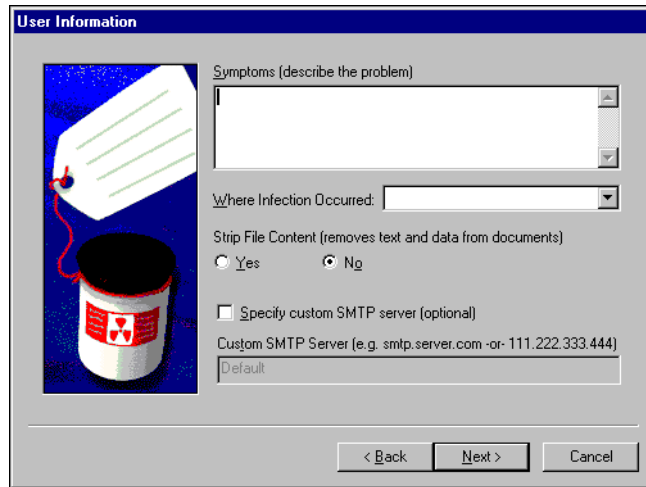
Submitting a file to SARC for analysis

The Quarantine includes the Scan and Deliver Wizard to simplify sending an item to SARC for analysis. When you click Submit Item, the Wizard analyzes the file and may recommend an action instead of delivering it to SARC. For example, the virus may be one that can already be eliminated with your current set of virus definitions. You can, however, override the recommendation and submit it.

To submit a file to SARC:

- 1 Open the Quarantine.
- 2 Select a file in the list of Quarantined items and click Submit Item.
- 3 Follow the directions in the Scan and Deliver Wizard to collect information and submit the file to SARC for analysis.

When the Wizard runs, there are two settings to cover special circumstances:

A screenshot of a Windows-style dialog box titled "User Information". On the left side, there is a graphic of a white tag with a red string tied to it, and a white bucket with a red radiation symbol. The main area of the dialog contains several fields and options: a text box labeled "Symptoms (describe the problem)", a dropdown menu labeled "Where Infection Occurred:", a section for "Strip File Content (removes text and data from documents)" with radio buttons for "Yes" and "No" (where "No" is selected), a checkbox for "Specify custom SMTP server (optional)", and a text box for "Custom SMTP Server (e.g. smtp.server.com -or 111.222.333.444)" with "Default" entered. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

Strip File Content: If checked, only the portion of a file that can be infected is sent to SARC. Check this if the file contains confidential data. This option also reduces connection time if a document file (which can be large) is submitted. The complete file, however, remains in the Quarantine.

Specify Custom SMTP Server:

Treating compressed files in the Quarantine

A compressed file may contain many individual files. For example, MYFILE.ZIP may contain the files: FILE1.DOC, FILE2.DOC, FILE3.TXT, FILE.EXE, and so on. Norton AntiVirus can detect viruses in the individual files within the compressed file, however it cannot repair or delete these files until you decompress (open up) the compressed file. Further, you cannot submit the complete compressed file to SARC for analysis; you must decompress the file first.

To decompress for repair or submission:

- 1 Double-click the Norton AntiVirus icon in the lower-right corner of the taskbar on your Windows desktop, then click Disable to turn Auto-Protect off temporarily.
- 2 Select the compressed file in the Quarantine and click Restore Item.
The compressed file is restored to its original location.
- 3 Use a program such as Norton Navigator, WinZip, or PKUNZIP to decompress the file.
- 4 Add the infected or potentially infected file to the Quarantine.
For more information, see [“Adding a file to the Quarantine manually”](#) on page 79.
- 5 In the Quarantine, select the file and click Repair Item.
- 6 Do one of the following:
 - If the file cannot be repaired, submit it to SARC for analysis.
 - If the repair is successful, the virus is removed and the file is restored to its original location. You can safely re-compress the file, if desired.
- 7 Double-click the Norton AntiVirus icon in the lower-right corner of the taskbar on your Windows desktop, then click the Enable button to enable Auto-Protect again.

Configuring the Quarantine

The Quarantine stores three sets of files:

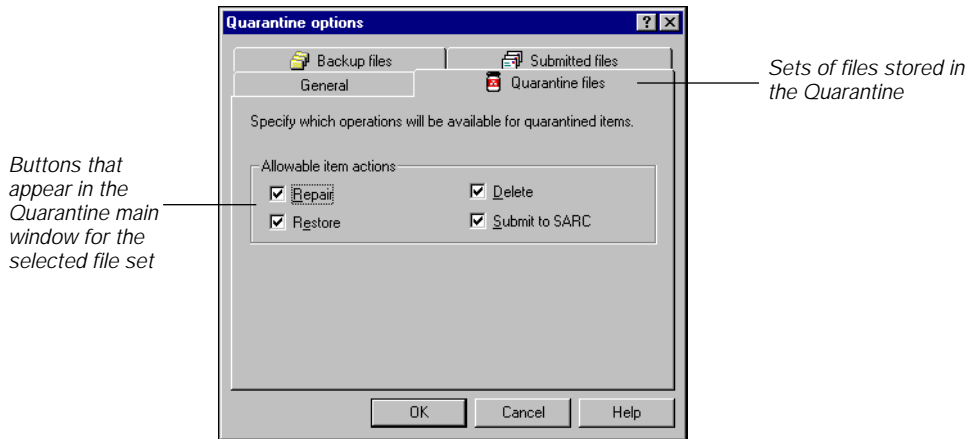
- Quarantined Items: Files isolated to prevent the spread of viruses.
- Backup Items: Backups of files that Norton AntiVirus saves before attempting a repair.
- Items Submitted To SARC: Files sent to SARC from the Quarantine for analysis.

You can specify which actions appear on the button bar in the Quarantine for each set of files. The preset actions are appropriate for most users and do not require change.

To specify allowable actions:

- 1 Open the Quarantine.
- 2 Select Options from the View menu.

Figure 6-3 Quarantine Options

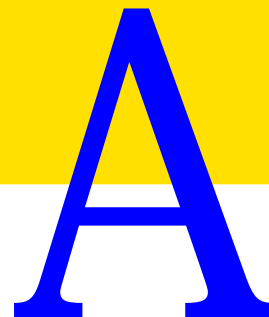


- 3 Click the Quarantine Files, Submitted Files, or Backup Files tabs and check which actions you want to permit for each file set.

If you do not want users to be able to change Quarantine options, you can set a password to prevent unwanted changes to Quarantine options.

To password-protect access to Quarantine settings:

- 1 Open the Quarantine.
- 2 Select Options from the View menu.
- 3 Click the General tab.
- 4 Check Enable Password and click Set Password.



About computer viruses

Protecting computers with properly configured antivirus software has become a requirement for everyday safe and secure computing. Although estimates of the actual number of detectable computer viruses vary dramatically, roughly 16,000 are believed to be in existence. This number reflects the fact that many identified viruses have multiple strains. A virus author can effectively create a new virus strain by changing as little as a single byte in an existing virus's code.

Virus authors often communicate through BBSs and Internet sites where they can chat about their activities and exchange tools and code. The majority of viruses, however, are not distributed beyond the boundaries of this virus-writing subculture. Only a fraction of the viruses in existence are released “in the wild”; that is, released in environments likely to be accessed by the general computing public.

In general, the level of talent of the average virus author is unimpressive, even when compared to the abilities of entry-level professional programmers. Many viruses are not written to deliberately interfere with a computer's operation, yet because the author has made so many errors in writing the virus, programs and data are subject to reckless destruction.

Whatever their source, the number of known viruses and infection incidents continues to increase:

- Many destructive viruses have already made their way into the wild.
- An ever-increasing number of virus types and strains continues to threaten the general computing population.

The potential costs related to viral damage are astronomically high.

What are computer viruses?

Computer viruses are, simply, 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 start-up area (boot record) or an executable file.

After a computer virus attaches to, or infects, a file or other part of your system, it spreads to neighboring items. Attaching itself to an item that is widely used by the general public or where file sharing is common, allows the virus to spread as widely as possible. The more successful the virus is in spreading, the greater its chances of survival.

There are many common misconceptions about what computer viruses actually do and what they are incapable of doing.

Viruses can infect...

- Program files, non-file areas used on computer start-up (boot records), and data files with macro capabilities
- Data disks and disks used to transfer programs
- Your computer when you download and use files from an online service
- A file before it is attached to an email message

Viruses cannot infect...

- Hardware, such as keyboards and monitors, graphic files, data files without macro capabilities, software items other than program files
- Write-protected disks
- Your computer when you read messages from an online service
- Text-based email messages

Trojan horse programs are often confused with computer viruses. Because they don't replicate and spread, they are not viruses.

A Trojan horse is a program that appears to serve some useful purpose or to provide entertainment. This guise encourages you to run it. But, like the Trojan horse of old, it also serves a covert purpose which may be to damage files or plant a virus on your computer.

Infection

Computer viruses are activated when you execute (or run) an infected program or start up a computer with infected boot records. Once activated, computer viruses spread in one of two ways depending on their design:

- Direct Action Infector
- Memory Resident Infector

A Direct Action Infector virus is activated when an infected file is executed. It takes control of the system before other software can load and looks for “clean” files to infect. When the infected program is closed, the virus stops infecting.

A Memory Resident Infector virus is much like a conventional terminate-and-stay-resident program (TSR). It hooks (takes over) the system when activated. A Memory Resident Infector maintains control of the system and continues to spread as you use your computer until memory is cleared (by rebooting), even if you close the infected program.

Trigger

Some, but not all, authors program their viruses to include an arbitrary incubation period. Once such a virus has made its way onto the computer, it waits to be activated by a trigger. Some of the many events that can act as triggers are a specific date, the count of sixty minutes after an infected program is executed, or the seventh program file that the virus program encounters. Other viruses use a random trigger.

Payload

Like a firearm, when the trigger is activated, an activity known as a payload occurs. Note that some viruses do not wait for a trigger, but deliver their payload whenever they are activated.

Some payloads are willfully destructive, such as those that format hard drives or corrupt files, while others are benign, doing little more than displaying a message on a computer screen. For example, a file infected with the Windows 95 Boza virus displays a lengthy message that begins with, “The taste of fame just got tastier!” (the payload) on the 30th day of any month (the trigger).

Viruses don’t necessarily let you know that they’re there, even after they do something destructive. For example, the Ripper virus will make random

changes to files on a disk so slowly that the changes go unnoticed by the average computer user.

Virus targets

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 which 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 greatest threat to the computing public. For example, Microsoft Word document and template files are susceptible to macro virus attacks. They spread very rapidly as infected documents are shared on networks or downloaded from Internet sites.

Each virus type, which uses a different mechanism to infect its particular target, is discussed in the following sections.

Program viruses

Like normal programs, program viruses must be written for a specific operating system. The vast majority of viruses are written for DOS but some have been written for Windows 3.x, Windows 95, and even UNIX.

All versions of Windows are compatible with DOS and can host DOS viruses with varying degrees of success. The following table describes how DOS program viruses behave in the different versions of Windows.

Table A-1

Windows version	Description of virus behavior
Windows 3.x	Most DOS viruses thrive in this environment because Windows 3.x uses DOS for all of its basic file functions.
Windows 95	Windows 95 is designed to be fully compatible with almost any older program, including program viruses. When a memory resident infector that attacks boot records is active, Windows 95 may display warnings during startup and your system's performance may degrade.
Windows NT	Windows NT provides the least degree of DOS compatibility, but still hosts program viruses. On Windows NT, memory resident infectors only infect and spread in a DOS session. If you close the DOS session, the virus is deactivated until you run an infected program in another DOS session. Also, because NT provides file security, program viruses can't infect or damage files you can't access.

Boot viruses

All hard and floppy disks have boot records, whether or not they also contain operating system files. A disk does not have to be bootable to be infected by a boot virus; data disks can contain boot viruses too. A typical way a computer gets a boot infection is to restart with an infected floppy disk inadvertently left in the drive. Even if the floppy is not a boot disk, the virus will activate and spread.

Unlike program viruses, almost any boot virus can infect DOS, Windows 3.x, Windows 95, Windows NT, and even Novell Netware systems. This is because they exploit inherent features of the computer (rather than the operating system) to spread and activate.

Many boot viruses assume the hard disk is using a normal DOS file system. Such an assumption is not always correct if you are using an operating system other than DOS or Windows 3.x. On Windows NT, for example, you can choose to use the NTFS file system instead of the DOS-compatible FAT file system. If a virus encounters a system using NTFS, it still successfully

infects the computer but it may accidentally damage some of your files or boot records (disk system areas) in the process.

When this happens, NT won't be able to start and you may need to reinstall Windows.

Another interesting aspect of Windows NT is that it will disable any boot viruses when it starts, assuming it can still start. This means that boot viruses can infect a machine running Windows NT but they can't spread to other systems while Windows NT is running. Don't, however, assume that the virus is benign. Every time you boot your system, the virus activates and has a chance to activate its trigger and deliver its payload. For example, on March 6th, the Stoned.Michelangelo virus writes random bytes to every cylinder on the hard drive, corrupting the original data. In a fraction of a second, key non-file areas used on computer start-up are the first to be wiped out in the process. It is virtually impossible to prevent the virus from destroying all data on the hard disk once the destructive trigger routine has activated.

Macro viruses

Many older applications had simple macro systems that let you record a sequence of operations within the application and associate them with a specific keystroke. Later, you could perform the same sequence of operations by hitting the specified key.

Newer applications provide much more complex macro systems. You can write entire macro-programs that run within the word processor or spreadsheet environment and are attached directly onto word processing and spreadsheet files. The ability to tote one or more macros around with a data file is a very powerful feature. Unfortunately, this ability also makes it possible to create macro viruses.

A typical chronology for macro virus infection begins when an infected document or spreadsheet is loaded; the application also loads any accompanying macros that are attached to the file. If one or more of the macros meet certain criteria, the application will also immediately execute these macros. Macro viruses rely upon this auto-execution capability to gain control of the application's macro system.

Once the macro virus has been loaded and executed, it waits for you to edit a new document, then re-activates. It attaches its virus macro programs onto the new document, then allows the application to save the document normally. In this fashion, the virus spreads to another file and does so

discretely; you have no idea of the infection. If this new file is later opened on another computer, the virus will once again load, be launched by the application, and find other unsuspecting files to infect.

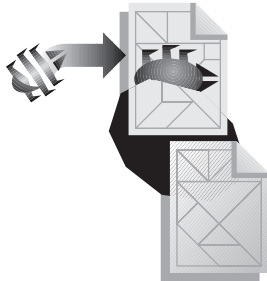
Finally, for macro viruses, the application serves as the operating system. A single macro virus can spread to any of the platforms on which the application is installed and running. For example, a single macro virus that uses Microsoft Word could conceivably spread to Windows 3.x, Windows 95, Window NT, and the Macintosh.

Virus technologies

Program and boot viruses are also categorized by the technology they use to replicate and attempt to avoid detection. Each is described in the following sections.

Stealth viruses

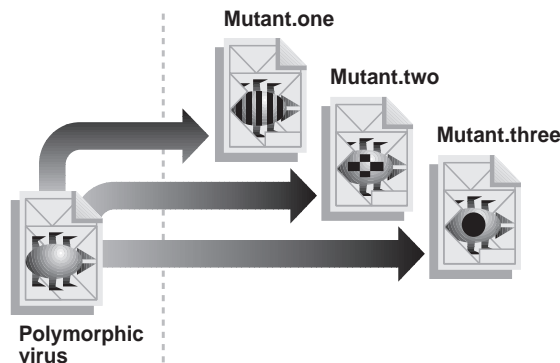
Stealth viruses actively seek to conceal themselves from attempts to detect or remove them. They use techniques such as intercepting disk reads to provide an uninfected copy of the original item in place of the infected copy (read-stealth viruses), altering disk directory or folder data for infected program files (size-stealth), or both.



For example, the Whale virus is a size-stealth virus. It infects .EXE program files and alters the folder entries of infected files when other programs attempt to read them. The Whale virus adds 9216 bytes to an infected file; because changes in file size are an indication that a virus might be present, the virus then subtracts the same number of bytes (9216) from the file size given in the directory/folder entry to trick the user into believing that the file's size has not changed.

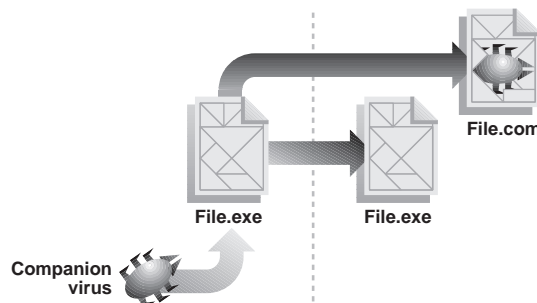
Polymorphic viruses

Most simple viruses attach identical copies of themselves to the files they infect. An antivirus program can detect the virus's code (or signature) because it is always the same and quickly ferret out the virus. To avoid such easy detection, polymorphic viruses operate somewhat differently. Unlike the simple virus, when a polymorphic virus infects a program, it scrambles its virus code in the program body. This scrambling means that no two infections look the same, making detection more difficult.



Companion viruses

A companion virus is the exception to the rule that a virus must attach itself to a file. The companion virus instead creates a new file and relies on a behavior of DOS to execute it instead of the program file that is normally executed.

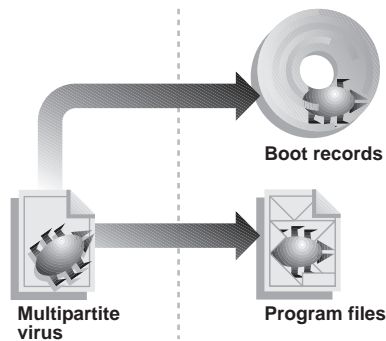


Companion viruses use a variety of strategies. Some companion viruses create a .COM file with a name identical to an existing .EXE file. For example, the companion virus might create a file named CHKDSK.COM and place it in the same directory as CHKDSK.EXE. Whenever DOS must

choose between executing two files of the same name where one has an .EXE extension and the other a .COM extension, it executes the .COM file.

Multipartite viruses

Multipartite viruses are both program and boot viruses. For example, if you run a word processing program infected with the Tequila virus, the virus activates and infects your hard disk boot record. Then, the next time you boot your computer, the Tequila virus activates again and starts infecting every program you use, whether it is on a hard or floppy disk.



Keeping your protection current

Norton AntiVirus, using techniques that defeat any attempts viruses may make to avoid detection, detects viruses based on their telltale virus signatures. This information is stored in the Norton AntiVirus virus definitions files. Your protection against viruses is only as current as the virus definitions files your Norton AntiVirus product is using.

To maximize your computer's protection against new viruses, you must regularly update your virus definitions files. You can get the new virus definitions files in a variety of ways, depending upon the product you are using. For detailed information and procedures, see [Chapter 4, "Keeping up with new viruses,"](#) on page 49.

The world of computer viruses is a dynamic one. Be sure to update your virus definitions files regularly.

Emergency recovery

When you can't start your computer

Boot sector viruses sometimes prevent you from starting up your computer at all. You won't be able to use Norton AntiVirus to diagnose and repair the problem. To help in this situation, Symantec provides an MS-DOS scanner. The Norton AntiVirus Scanner (NAVDS.EXE) is available for download from <http://www.symantec.com>.

To use NAVC in an emergency situation, you must start your computer from an MS-DOS boot disk, not a Windows NT boot disk. The README.TXT file that accompanies NAVC gives detailed recovery procedures.

Using command-line switches

NAVWNT.EXE, the Windows NT scanner, can be run with command-line switches to override configuration settings. When scanning using command-line switches, Norton AntiVirus runs minimized, but will pop open on your screen if a virus is found.

Some switches are used alone, while others are followed by a parameter, either a plus (+) or minus (-) sign. You can use more than one switch and more than one parameter on a command line. The vertical bar symbol (|) means that you should use either parameter, but not both. Do not type the brackets around the parameters on the command line. Use the following syntax to run NAVWNT with switches:

NAVWNT [pathname] [options]

pathname	Any drive, folder, file, or combination of these is scanned. To scan multiple items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files, for example, NAVWNT A: C:\MYDIR*.EXE
/A	All drives, except drives A: and B:, are scanned. Network drives are scanned if the Allow Network Scanning option is selected in the Scanner Advanced Settings dialog box.
/L	All local drives, except drives A: and B:, are scanned.
/S[+ -]	Enables (+) or disables (-) scanning of subfolders for any folders specified in the pathname. S+ is the default.

<code>/B[+ -]</code>	Enables (+) or disables (-) scanning of boot records, for example, NAVWNT A: /B+ or NAVWNT A: /B- (default is the Scanner options setting).
<code>/BOOT</code>	Only the boot records of the specified drives are scanned.
<code>/NORESULTS</code>	No scan results are displayed on screen (for unattended or scheduled scans).

The following examples demonstrate command-line syntax for a variety of situations:

- To scan all .EXE files in your WIN32APP folder and descending subfolders, type the following:
`NAVWNT C:\WIN32APP*.EXE`
- To scan all .EXE files in your WIN32APP folder only:
`NAVWNT C:\WIN32APP*.EXE /S-`
- To scan a folder and descending subfolders with long filenames (LFN), use double quotes:
`NAVWNT "C:\Program Files"`
- To scan a drive and a folder on another drive:
`NAVWNT C: D:\NEWFILES`
- To scan a folder on the network drive P: called PROGRAMS but none of its subfolders:
`NAVWNT P:\PROGRAMS /S-`
- To scan only the boot records of drives C: and A:
`NAVWNT C: A: /BOOT`
- To use the Windows NT Scheduler Service to initiate an automatic scan of all local drives (except the A: and B: drives) at 5:30 P.M. every weekday, enter the following command on one line.
For Windows NT 4.0:
`at 17:30 /interactive /every:M,T,W,Th,F
"c:\Program Files\NAVNT\NAVWNT" /L /NORESULTS`
For Windows NT 3.51:
`at 17:30 /interactive /every:M,T,W,Th,F
"c:\Win32app\NAVNT\NAVWNT" /L /NORESULTS`

The `/interactive` parameter must be used when scheduling Norton AntiVirus scans. For more information on using the Scheduler Service, See your Windows NT documentation.

G L O S S A R Y

application	<i>See</i> program.
(to) boot	To start the computer.
bootable disk	A disk that contains the operating system necessary to start, or boot, the computer.
boot record	The first physical sector on a floppy disk or the first logical sector of a hard disk partition. It identifies the disk's architecture (sector size, cluster size, and so on). It also contains the boot record program.
boot record program	The program that is responsible for loading the operating system.
boot virus	A virus that infects the boot record program on both hard and floppy disks and/or the master boot record program on hard disks. A boot virus loads into memory before the operating system, taking control of your computer and infecting any floppy disks that you access.
bulletin board system (BBS)	An on-line service that allows messaging, electronic mail, and file transfer between computer users via modem.
.COM file	<i>See</i> executable file.
command-line switch	An option that controls the operation of a program. Switches can be used when a program is executed from the operating system prompt or through the RUN command in Windows.
compressed file	A single file or series of files that have been compressed into one file using a compression utility such as PKZIP or LHARC.
data file	A file that is created by or associated with an application and contains no executable code.
directory	<i>See</i> folder.
download	To transfer a file from one computer system to another through a modem. Most frequently used when referring to the act of transferring a file from a bulletin board system.

dropper	A program that installs a virus on your computer. Droppers are not viruses, they are trojan horse programs. <i>See also</i> trojan horse.
exclusion	An item that you have instructed Norton AntiVirus not to scan.
.EXE file	<i>See</i> executable file.
executable file	A file containing a program that can be launched. Executable files generally have the following extensions: COM, EXE, OVR, OVL, DRV, BIN, or SYS.
folder	A portion of a disk that you designate to store information about files. Folders make it easier for you to organize the files on your disk. Also called a directory.
infected file	A file that contains a virus.
known virus	Any virus that Norton AntiVirus can detect and identify by name.
.LHA file	A series of files that have been compressed into one file using the LHARC utility.
macro virus	A virus that infects document files or spreadsheets. Generally, a macro virus is executed when an infected document is opened, saved, or closed, and spreads to other documents. Macros, which are small programs associated with document files, are used to automate tasks.
master boot record (MBR)	The first physical sector on a hard disk. It contains the master boot record program and information on how a hard disk is partitioned.
master boot record program	The program that is responsible for directing the computer to load the boot record program from the bootable hard disk.
memory-resident program	<i>See</i> terminate-and-stay-resident program.
multipartite virus	A virus that infects and spreads from both program files and boot records.
operating system	The master control program that is loaded into memory when you start up or boot your computer. It controls and manages all computer operations and programs.

partition table	A table in the master boot record of a hard disk that specifies how the disk is set up, such as the size and location of the partitions, which operating system each partition uses, and which partition the computer will boot from.
pathname	The location of a file or folder on a disk. For example, if a file named QTR1.DOC is stored in the folder OFFICE on drive C:, the pathname for the file is C:\OFFICE\QTR1.DOC.
polymorphic virus	A type of virus that changes its telltale code segments so that it “looks” different from one infected file to another, thus making detection more difficult.
program	An executable file or group of files written for a specific purpose such as word processing or creating a spreadsheet.
program virus	A virus that infects executable program files, such as .COM, .EXE, .OVL, .DRV (driver), and .SYS (device driver) files.
RAM	<i>See</i> random access memory.
random access memory (RAM)	The computer’s working memory that determines the size and number of programs that can be run at the same time, as well as the amount of data that can be processed instantly.
read-only	Refers to a disk or file containing data that can be read, but cannot be written to or deleted.
reboot	To restart your computer. <i>See also</i> warm boot and cold boot.
repair	To remove a virus from a file and return the file to its original, uninfected state.
scan	The systematic search for viruses that is performed by Norton AntiVirus.
stealth virus	A virus that actively seeks to conceal itself from discovery or defends itself against attempts to analyze or remove it.
subdirectory	<i>See</i> subfolder.
subfolder	A folder within a folder.
system disk	<i>See</i> bootable disk.
system files	The files that make up the operating system.

taskbar	The desktop component in Windows NT 4.0 that gives access to the Start menu and currently running programs. Auto-Protect and the Norton Scheduler place icons on the taskbar to remind you they are enabled.
trojan horse	A program that promises to be something useful or interesting (like a game), but covertly may damage or erase files on your computer while you are running it. Trojan horses are not viruses because they don't replicate and spread.
virus	A self-replicating program written intentionally to alter the way your computer operates without your permission or knowledge.
virus definition	Virus information that allows Norton AntiVirus to recognize and alert you to the presence of a specific virus.
write-protected disk	A disk that cannot be written to. Write-protecting disks prevents viruses from infecting them. To write-protect a 5.25" disk, cover the notch on the side of the disk with an adhesive label (usually a tab included with boxes of disks). To write-protect a 3.5" disk, slide the lever on the back of the disk to uncover the hole through the disk.
.ZIP file	A series of files that have been compressed into one file (usually with a .ZIP file extension) using PKZIP.

I N D E X

A

- access privileges
 - boot record, 22
 - file, 22
 - folder, 22
- Activity Log
 - completion of scans, 69
 - customizing, 69–70
 - filtering events, 35
 - finding files requiring replacement, 44
 - known virus detections, 69
 - limiting size of, 70
 - logging events, 69
 - printing events, 34
 - setting file size, 70
 - types of events, 69
 - viewing all entries in, 34
 - virus list changes, 69
- Activity Log Filter dialog box, 35
- Activity Log Settings tab, 69
- Add Event dialog box, 30
- adding
 - exclusions, 66
 - program file extensions, 64
- advanced scanning options, 60–61
- alerts
 - add message to, 68
 - Auto-Protect, 18, 43–44
 - customizing, 67–68
 - customizing response option, 59–60, 73–74
 - enabling audible alarm, 68
 - sending over Novell NetWare networks, 68
 - situations triggering, 43
 - virus found alert, 44
- Alerts tab, 67, 68
- audible alarms, enabling, 31, 52, 68
- automatic functions, Norton AntiVirus, 9
- automatic protection, 32–33

- Auto-Protect feature
 - configuring for Internet protection, 35
 - customizing, 71–74
 - described, 16
 - eliminating viruses detected by, 43–44
 - enabling, 32–33
 - Windows 95, 81
 - Windows NT, 33
 - floppy disks, 74
 - loading automatically, 33
 - program files, 71–74
 - temporarily disabling, 32–33
 - virus found alert, 44
- Auto-Protect Settings tab, 71
- avoiding viruses, 23

B

- backup file extensions, setting, 70
- boot records
 - access denied, 28
 - bypass scan of, 28
 - manual scan of, 58
 - repairing automatically, 59
 - repairing infected, 59
 - unsuccessful repairs to, 45
- boot viruses
 - checking floppy disks for, 74
 - described, 54, 87
 - spread mechanism, 87
 - viewing lists of, 54

C

- command buttons, 42–43
 - See also* Problems Found dialog box
- command-line switches, 95–97
- common problems, resolving, 46
- common viruses
 - defined, 54
 - viewing lists of, 54

- companion viruses, described, 90
- compressed files
 - manual scan of, 58
 - removing viruses from, 46
- computer virus
 - avoiding, 23
 - definition, 14
 - detecting, 39
 - dual boot exposure, 22
 - infection cycle, 14–15
 - scanning procedures, 25–27
 - types, 19
- computers
 - protecting against viruses, 13
 - security considerations, 21
- Continue button, 43
- copying files from floppies, 45
- customizing
 - Activity Log, 69–70
 - alerts, 67–68
 - backup file extension, 70
 - Exclusions List, 65
 - how to respond when virus is found, 59–60
 - manual scans, 57–60
 - virus alerts, 59–60
 - what to scan, 57–61

D

- Delete button, 43
- deleting
 - files
 - automatically, 59
 - in response to alerts, 44
 - irreparably damaged, 45
 - program file extensions, 65
- denying access to infected program files, 73
- detecting viruses
 - Auto-Protect scans, 39
 - manual or scheduled scans, 39
 - methods, 15
- drives, preselecting for scans, 61

E

- editing
 - custom alert message, 67
 - exclusions, 67
- Emergency recovery, 93
- enabling
 - audible alarms, 31, 52
 - Auto-Protect feature, 32–33
 - scheduled virus scans, 31, 52
- enabling virus protection
 - Windows 95, 81
 - Windows NT, 33
- Exclude button, 43
- excluding subfolders from scans, 66
- exclusions
 - adding manually, 66
 - defined, 65
 - modifying, 67
 - removing from Exclusions List, 66
- Exclusions List, 65
 - modifying, 65
 - removing exclusions from, 66
 - viewing, 65
- Exclusions tab, 66
- exiting Norton AntiVirus, 24

F

- files
 - backup options, 70–71
 - deleting automatically, 59
 - deleting infected, 44
 - denying access to infected, 73
 - re-infected by removed viruses, 46
 - removing viruses from compressed, 46
 - requiring replacement, finding, 44
 - scanning all, 62
 - selecting for scanning, 62–63
 - unsuccessful repairs to, 45–46
- filtering Activity Log entries, 34, 35
- floppy disks
 - monitoring for viruses, 74
 - scanning for viruses, 60–61, 74

H

help during install, 11

I

immediate notification of viruses, 61

infected files and boot records

- deleting, 44

- deleting automatically, 59

- removing viruses from compressed, 46

infected files. *See* files

infections. *See* virus attacks

Info button, 43

installing

- Norton AntiVirus, 9–12

- questions, 11

- system requirements, 10

- uninstalling, 12

Internet

- browsers, 36

- configuring Auto-Protect for, 35

K

known viruses

- See also* computer virus; viruses

- defined, 16

- viewing a list of, 53

- viewing report of detections, 34

M

macro viruses

- defined, 19

- described, 88

manual scans, 57–59

- about, 16

- all files, 58

- compressed files, 58

- customizing, 57–60

- master boot record, 58

- program files, 58

master boot record, manual scan of, 58

MS-DOS scanner, 22

multipartite viruses

- defined, 54

- described, 91

- viewing lists of, 54

N

network alerts

- sending to Norton AntiVirus for

 - NetWare NLM, 68

- setting alert options, 68

network drives

- restrictions on scanning, 62

- scanning, 62

New Exclusion dialog box, 66

Norton AntiVirus

- automatic functions, 9

- described, 9

- exiting, 24

- installation requirements, 10

- installing, 9–12

- Internet browsers and, 36

- Netscape and, 36

- starting, 24

- uninstalling, 12

- updating, 9

- virus protection technologies, 16–18

Norton AntiVirus Scanner for DOS, 93

Norton AntiVirus Scanner, scheduling, 29

NORTON PROGRAM SCHEDULER (Windows

- Start menu) command, 29, 51

O

online help

- accessing, 25

- Auto-Protect feature, 25

P

password protection

- changing password, 76

- custom, 75

- password protection (*continued*)
 - maximum, 75
 - removing password, 76
 - setting, 74–76
- Password Settings tab, 75
- payload, virus, 85
- polymorphic viruses
 - defined, 54
 - described, 90
 - viewing lists of, 54
- preventing virus attacks with Norton AntiVirus, 15
- printing
 - Activity Log, 34
 - Virus List, 55
- Problems Found dialog box, 42
- program file extensions
 - adding new, 64
 - deleting, 65
 - resetting list of, 65
 - specifying for scans, 58, 63–65
 - viewing current, 63–64
- Program File Extensions dialog box, 64
- program files
 - Auto-Protect scans of, 72
 - deleting after virus detection, 73
 - failure to execute after repair, 47
 - manual scans of, 58
 - removing viruses from, 72–74
- program viruses
 - defined, 54
 - described, 86
 - spread mechanisms, 86
 - viewing lists of, 54
- protection, automatic, 9

R

- recovering from virus emergencies, 15
- removing
 - program file extensions, 65
 - viruses
 - from compressed files, 46
 - from files and boot records, 46
- repair attempts, unsuccessful, 93
- Repair button, 43
- Repair Wizard, 40
 - deleting a file, 41
 - eliminating viruses automatically, 39
 - eliminating viruses manually, 39
- repairing files and boot records
 - automatically, 73
 - failure to execute after, 47
- reports, viewing activity, 34–35
- requirements, installation, 10

S

- Scanner Advanced Settings dialog box, 61
- Scanner tab, 57
- scanning for viruses
 - all files, 62
 - floppy disks, 60–61, 74
 - network drives, 61, 62
 - program files, 62
 - specifying program file extensions, 62–65
 - stopping scans in progress, 61
- scans
 - automatic, 71–73
 - Auto-Protect, 16
 - excluding subfolders from, 66
 - manual, 16, 57–59
 - preselecting drives, 61
 - scheduled, 16
 - viewing date/time occurred, 35

- Scheduler
 - accessing, 29
 - scheduling scans, 30
- scheduling automatic scans, 29–32
- security considerations, Windows NT, 21
- Set Password dialog box, 75
- stealth viruses
 - defined, 54
 - described, 89
 - viewing lists of, 54
- Stop button, 43
- system files, unsuccessful repairs to, 45
- system requirements, 10

T

- trigger, virus, 85

U

- uncompressing files for repair
 - Windows 95, 81
- uninstalling Norton AntiVirus, 12
- update, virus definitions, 17
 - automatic, 49–50
 - sources, 53
- updating Norton AntiVirus, 9

V

- viewing
 - Activity Log, 34–35
 - Exclusions List, 65
 - program file extensions, 63
 - scheduled scans, 30
 - virus list, 53–55
- virus attacks
 - emergency recovery from, 93
 - mechanisms of, 15
 - preventing, 23
 - sources of, 15
- virus definitions file
 - installing new, 53
 - reasons for updating, 16, 17

- virus definitions, updating, 49–53
- virus found alert, 44
- virus infection cycle, 14–15
- virus list
 - updating, 49
 - viewing and printing, 53–55
- Virus List dialog box, 53
- virus protection
 - enabling
 - Windows 95, 32, 33, 81
 - Windows NT, 33
- virus signatures, 16, 17
- viruses
 - defined, 84
 - files re-infected by removed, 46
 - payloads, 85
 - searching for names of, 55
 - sources of, 15
 - spread mechanisms, 15
 - targets of infection, 86
 - triggers, 85
 - viewing names and descriptions of, 53–55

W

- Windows NT
 - security, 21
 - virus risk, 19–21