

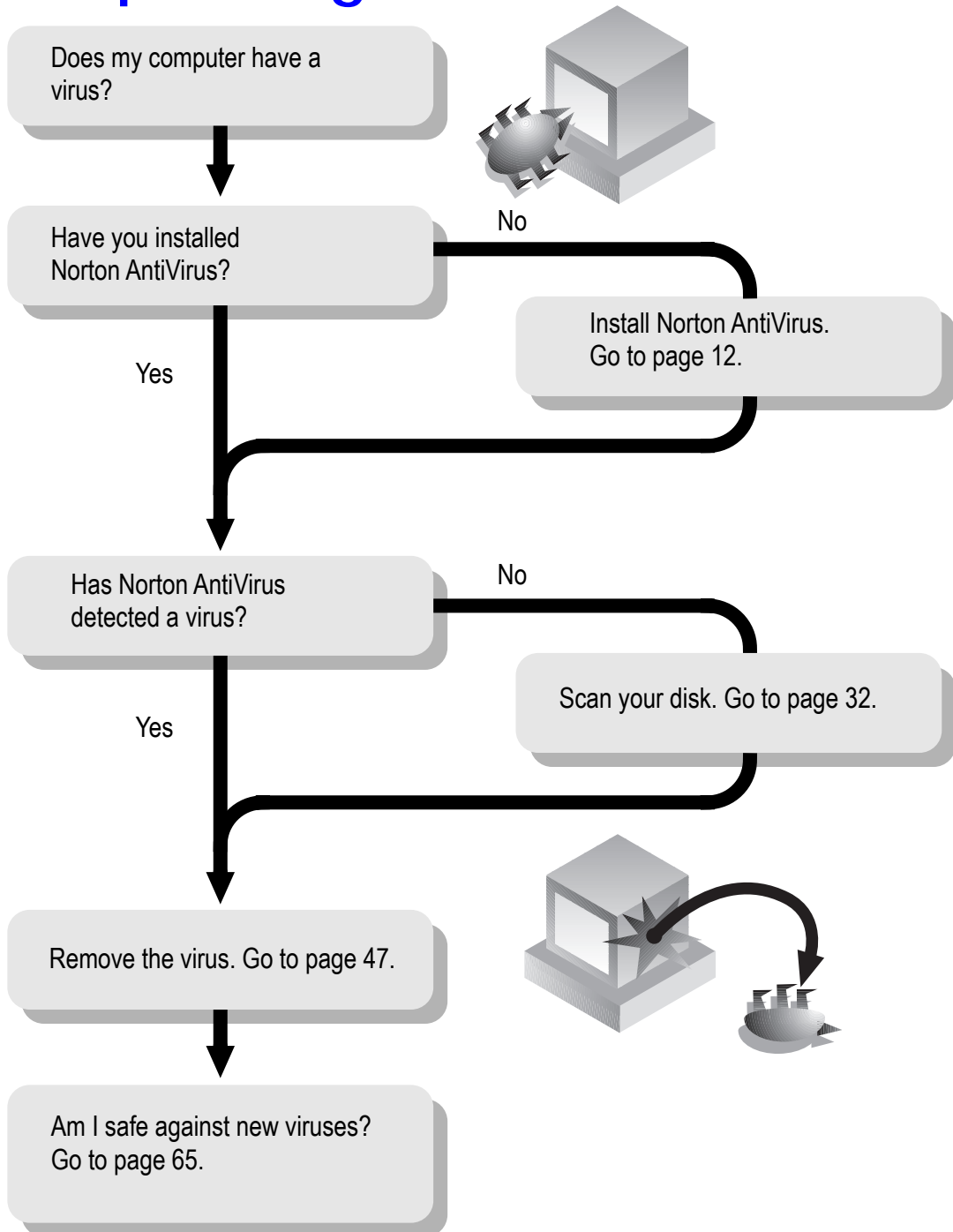
Reference Guide

NORTON

AntiVirus™

VERSION 5.0

Help! I've got a virus!



Norton AntiVirus[™] for Windows[®] 95/98 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 THE 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 (collectively 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 that number of copies of the appropriate titles of the software as have otherwise been licensed to you by Symantec under a Symantec Volume Incentive or Value License, provided that the number of copies of all such titles in the aggregate will not exceed the total number of copies so indicated on such Volume Incentive or Value license;
- (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 printed 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;
- (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;
- (v) use the server based software products included with the Software if you have not licensed the Norton AntiVirus Solution for server-based products;
- (vi) use the suite based software products included with the Software if you have not licensed the Norton AntiVirus Solution Suite;
- (vii) use other than the Macintosh versions of the software if you have only licensed the Macintosh versions of the software; or
- (viii) use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version.

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 Service, 175 W. Broadway, Eugene, OR 97401. Symantec, the Symantec logo, Norton AntiVirus, SAM, and SAM Administrator are U.S. registered trademarks of Symantec Corporation. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. NetWare is a registered trademark of Novell, Inc. Other brands and products are trademarks of their respective holder/s. © 1998 Symantec Corporation. All rights reserved. Printed in the U.S.A. Manufactured under an NSAI registered ISO 9002 quality system. 21088 2/98 07-70-00896

SYMANTEC SOFTWARE LICENSE ADDENDUM

Notwithstanding any of the terms and conditions contained in the Symantec Software License, you may make and use up to that number of copies of the Software that is indicated on the License Authorization Coupon contained in your box. The coupon will constitute proof of your right to make and use such additional copies.

C O N T E N T S

Installation

Requirements for installing	11
Installing Norton AntiVirus for Windows 95/98	12
Questions when installing	12
Testing the Norton Rescue Boot Disk	13
If you didn't create Rescue Disks	14
Uninstalling Norton AntiVirus for Windows 95/98	14

Quickstart

Making sure you're protected	16
------------------------------------	----

Chapter 1 About Norton AntiVirus

Is my computer protected against viruses?	19
What is a computer virus?	20
Virus infection cycle	21
How Norton AntiVirus protects you	23
Manual scans	24
Scheduled scans	25
Startup scans	25
Auto-Protect	25
Inoculation	25
Virus definitions files	26
How Norton AntiVirus warns you	26

Chapter 2 Using Norton AntiVirus

Tips to avoid viruses	29
Starting and exiting Norton AntiVirus	30
Getting help	31
Scanning for viruses	32
Turning Norton AntiVirus Auto-Protect off temporarily	35
Bypassing startup protection	36
Inoculating boot records	37
Viewing the Activity Log	37
Creating a rescue disk set	39
Scheduling virus scans	40
Scheduling scans for Windows 98	40
Scheduling scans for Windows 95	41

Chapter 3 Eliminating viruses

Eliminating viruses detected during scans	47
Responding to Inoculation alerts	50
Command buttons	51
Eliminating viruses detected by Auto-Protect	53
Responding to Auto-Protect virus in memory alerts	55
Responding to Auto-Protect virus found alerts	56
Responding to Auto-Protect virus-like activity alerts	57
Eliminating viruses detected during startup scans	59
Responding to startup scan virus in memory alerts	59
Responding to startup scan virus found alerts	60
What to do if repair is unsuccessful	60
Infected files	61
Compressed files	62
Hard disk master boot record or boot record	62
Floppy disk boot record	63
System file	63

Chapter 4 Keeping up with new viruses

Automatically updating virus definitions	65
Using LiveUpdate Email	67
Scheduling an automatic LiveUpdate in Windows 98	67
Scheduling an automatic LiveUpdate in Windows 95	68
Manually updating virus definitions	69
Viewing the Virus List	70

Chapter 5 Customizing Norton AntiVirus

Customizing manual scan options	73
Notes on scanning network drives	78
Selecting which files to scan	78
Specifying program file extensions	79
Managing exclusions	81
Customizing alerts	84
Sending network alerts	85
Customizing the Activity Log	86
Setting general scanning options	88
Customizing automatic protection	89
Auto-Protecting program files	89
Monitoring for virus-like activities	92
Auto-Protecting floppy disks	94
Customizing startup protection	95
Customizing inoculation	96
Setting password protection	98

Chapter 6 Managing the Quarantine

Using the Quarantine	101
Adding a file to the Quarantine manually	103
Submitting a file to SARC for analysis	104
Treating compressed files in the Quarantine	105
Configuring the Quarantine	105

Appendix A About computer viruses

What are computer viruses	108
Virus targets	110
Program viruses	110
Boot viruses	111
Macro viruses	112
Virus technologies	113
Keeping your protection current	115

Appendix B Using your Norton AntiVirus Rescue Disks

Removing viruses from a shutdown computer	117
Restoring your hard disk	118

Appendix C Using command-line switches

NAV DX.EXE	121
NAVW32.EXE	124
RESCUE.EXE	126

Appendix D System messages

Messages and their meanings	127
-----------------------------------	-----

Appendix E Troubleshooting

Solutions to common problems	135
------------------------------------	-----

Glossary

Index

Installation

When you install Norton AntiVirus exactly as directed by the on-screen messages, you will have complete virus protection as soon as you restart your computer. This includes:

- Norton AntiVirus loaded automatically each time you start your computer.
- Rescue Disks to protect you in case you can't start your computer.
- An automatic scan of your disks once per week to ensure they stay virus-free.
- Protection when you download files from the Internet

Requirements for installing

Your minimum computer requirements are:

- 486 IBM or compatible PC
- 8 MB of RAM (16 MB or higher recommended)
- Microsoft Windows 95 or 98
- 24 MB of free hard disk space

You also must have:


- Three 1.44 MB floppy disks and three disk labels (for Rescue Disks)

WHY? The last step of Install asks you to create Rescue Disks. These Rescue Disks are an important part of your virus protection. For example, they allow you to safely restart your computer if it is halted due to a virus in memory.

Installing Norton AntiVirus for Windows 95/98

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

To install Norton AntiVirus for Windows 95/98:

- 1 Do one of the following:
 - To install from a CD, 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 12](#).
- 3 Test the Norton Rescue Boot Disk that you created during installation. See [page 13](#) for testing details.

Questions when installing

Norton AntiVirus helps you install by giving you on-screen directions and offering the recommended actions. You are asked to make the following choices.

What the choices are	What you should do	Why
Select the folder for Norton AntiVirus.	Accept the preset choice: <code>C:\Program Files\Norton AntiVirus</code>	The choice is there for unusual circumstances.
Schedule weekly scans of your local hard disks that run automatically.	Leave this checked.	A weekly scan makes sure your disks stay virus-free.

What the choices are	What you should do	Why
Enable Auto-Protect.	Leave this checked.	Auto-Protect constantly monitors your computer to make sure a virus does not gain entry.
Scan at startup.	Leave this checked.	Makes sure critical system files are virus-free every time you start up.
Run LiveUpdate after installation.	Leave this checked if you have a modem or an Internet connection.	LiveUpdate connects to a special Symantec site and updates Norton AntiVirus automatically to protect you against newly discovered viruses.
Do you wish to create Rescue Disks?	We strongly recommend that you create the Rescue Disks.	Rescue Disks can save you from disaster if your computer becomes infected with certain types of viruses.
Scan for viruses after installation.	Leave this checked.	Makes sure that your computer is virus-free.
Norton AntiVirus has detected a Netscape browser. Do you want to install plug-ins?	Choose Yes.	This option allows Norton AntiVirus to scan files for viruses when you download using a Netscape browser.
Would you like to restart your computer?	Select Yes, I want to restart my computer now.	When your computer restarts, you are fully protected against viruses.

Testing the Norton Rescue Boot Disk

The Norton Rescue Boot Disk starts your computer in emergency situations. However, Norton AntiVirus cannot create a boot disk for all hard drives automatically. You should always test your Norton Rescue Boot Disk to make sure that it works, before you need it.

To test your Norton Rescue Boot Disk:

- 1 Click Start on the Windows taskbar, click Shut Down, select Shut Down Your Computer, and click OK.

- 2 Turn off the power.
- 3 Insert the first disk of your Norton AntiVirus rescue disk set, labelled “Norton Rescue Boot Disk,” in the A: drive, then restart your computer.
- 4 After your computer starts, type `TEST` and press Enter.
A screen message reports whether your Norton Rescue Boot Disk works properly.

Note: Your Norton Rescue Boot Disk doesn't work? See [page 135](#).

- 5 Remove the Rescue Disk and restart your computer.
Because you didn't start Windows for the test, you don't have to perform the usual Windows Shutdown.
- 6 Slide open the plastic tab on the back of the disk to write-protect it. This prevents you from accidentally changing the data stored on the disks.

If you didn't create Rescue Disks

If you didn't create Rescue Disks during installation, create them now. You need three 1.4 MB floppy disks and three disk labels.

To create Rescue Disks:

- 1 On the Windows taskbar, click Start, point to Programs, point to Norton AntiVirus, and then click Rescue Disk.
- 2 Follow the on-screen instructions.
- 3 Test your Norton Rescue Boot Disk.
See “[Testing the Norton Rescue Boot Disk](#)” on page 13.

Uninstalling Norton AntiVirus for Windows 95/98

To uninstall Norton AntiVirus:

- Click Start on the Windows taskbar, point to Programs, point to Norton AntiVirus, and then click Uninstall Norton AntiVirus.

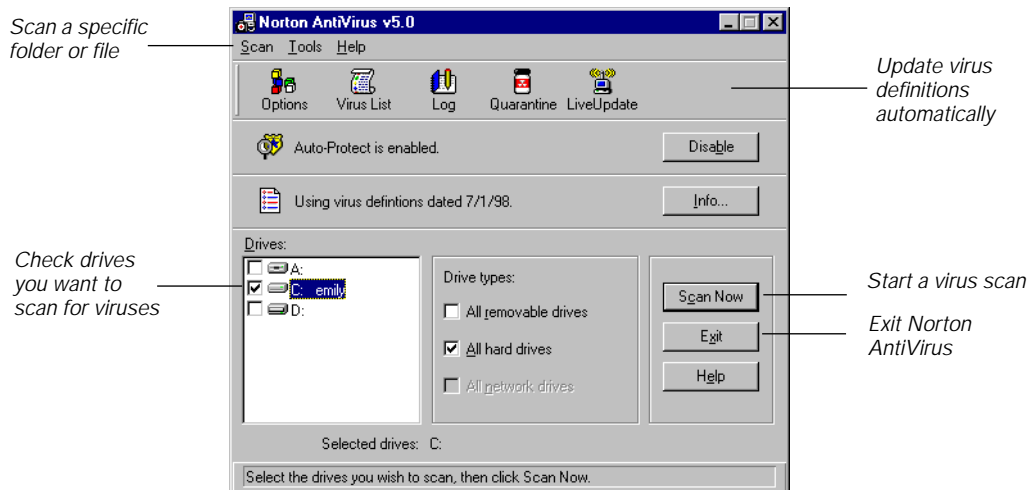
Quickstart

To start Norton AntiVirus:

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

The Norton AntiVirus main window appears.

Figure 1 Norton AntiVirus main window



To scan one or more drives:

- In the Norton AntiVirus main window, check specific drives to scan in the Drives list box and click Scan Now.

To scan a specific file or folder:

Do one of the following:

- In the Norton AntiVirus main window, choose File from the Scan menu.
- In the Norton AntiVirus main window, choose Folders from the Scan menu.

To get help using Norton AntiVirus:

Do one of the following:

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

If you performed a complete installation and accepted the recommended options, Auto-Protect and Startup scans are already enabled and a scan of your hard disks is scheduled to run automatically once per week.

To make sure Auto-Protect is always loaded:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Auto-Protect tab.
- 3 Check Load Auto-Protect At Startup.
- 4 Click OK.

To make sure Startup scans are enabled:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Startup tab.
- 3 Check the following options in the What To Scan group box:
 - Memory
 - Master Boot Record
 - Boot Records
 - System Files
- 4 Click OK.

Making sure you're protected

To keep your computer free of viruses, follow these rules:

- Update your virus definitions files monthly so that you maintain maximum protection against newly identified viruses. See [Chapter 4, "Keeping up with new viruses,"](#) on page 65 for directions.
- Scan all hard disk drives at least once per week to verify they are virus-free.

- Scan all new files and floppy disks before first use.
- Create a Norton AntiVirus Rescue Disk set, which you use to restore a damaged hard disk and recover from certain boot viruses. See “[Creating a rescue disk set](#)” on page 39 for more information.
- Make periodic backups of your hard disk.
- Buy legal copies of all software you use and make write-protected backup copies.

About Norton AntiVirus

Norton AntiVirus for Windows 95/98 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 for Windows 95/98 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 ever found, Norton AntiVirus guides you through the process of eliminating it.

If computers are a mystery to you, don't worry. The Norton AntiVirus for Windows 95/98 preset options balance efficiency with maximum protection; you do not need to change anything. Simply install Norton AntiVirus and you are immediately protected from computer viruses.

Here's what Norton AntiVirus does automatically:

- Checks system files and boot records for viruses at system startup.
- Checks programs for viruses at the time you use them.
- Scans your computer for viruses once per week.
- Monitors your computer for activity that might indicate the work of a virus in action.
- Checks floppy disks for boot viruses when you use them.
- Checks files downloaded from the Internet for viruses.

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 at least once per month.
- Submit suspicious files to the Symantec AntiVirus Research Center (SARC) 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 is activated and attaches itself to yet 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. Most 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 what's stored on them.

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

- Program viruses: Infect executable files, such as word processing, spreadsheet, computer game, or operating system programs.
- Boot viruses: 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.
- Macro viruses: Infect data files with macro capabilities. In many word processing and spreadsheet applications, you can record a macro that stores a series of actions. Later, you can run the macro

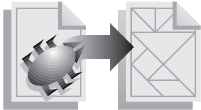
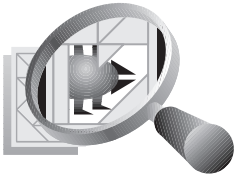
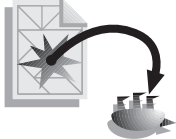

and automatically repeat the same actions. For example, Microsoft Word document and template files are susceptible to macro virus attacks.

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 or quarantined, it continues to infect other files and possibly damage data on your disks. Table 1-1, “Details of the virus life cycle,” on page 22 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 bargains (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 Open infected document or spreadsheet
	Spread	Share disk or infected program Log on to network
Detection 	Observation	Strange system behavior Files missing or programs not working
	Utility	Virus detected by anti-virus software
Recovery 	Cleanup	Reinstall programs from master disks Repair files with anti-virus 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

All computer viruses, irrespective of their targets, fall naturally into two groups:

- **Known viruses:** 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 eradicate 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 file at least once per month so that Norton AntiVirus has the information it needs to find all known viruses. See [Chapter 4, "Keeping up with new viruses,"](#) on page 65 for instructions on getting the latest virus definitions files.

- **Unknown viruses:** An unknown virus is one that does not yet have a virus definition. Norton AntiVirus includes an advanced heuristic technology called Bloodhound to detect unknown program and macro viruses. Bloodhound isolates and locates the various logical regions of a file and then analyzes the program logic for virus-like behavior. Bloodhound detects a very high percentage of unknown viruses.

In addition, Norton AntiVirus detects unknown viruses by monitoring activity on your computer for behaviors that viruses typically perform. When a suspicious activity is detected, Norton AntiVirus prevents the action from continuing.

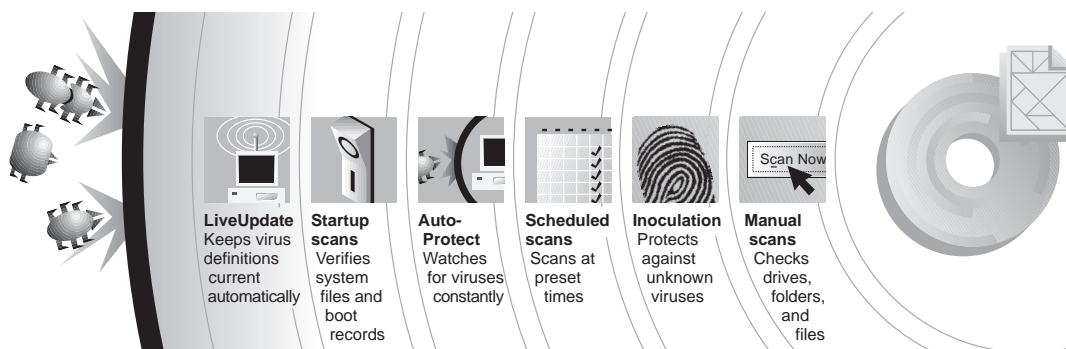
Sometimes Norton AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions. Or, you have a file you think is infected that is not being detected. The Norton AntiVirus Quarantine safely isolates virus-infected files on your computer. A virus in a quarantined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

From the Quarantine, a file can be sent over the Internet directly to the Symantec AntiVirus Research Center (SARC) for analysis using the Scan and Deliver Wizard. 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. For more information, see [“Submitting a file to SARC for analysis”](#) on page 104.

Symantec engineers have developed several complementary technologies to keep your computer virus-free. Figure 1-1, “Norton AntiVirus technologies,” illustrates how the Norton AntiVirus technologies work together to detect, eliminate, and prevent viruses—whether known or unknown—from gaining entry to your computer.

Figure 1-1 Norton AntiVirus technologies



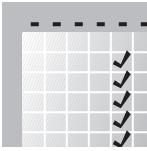
The scanner, which examines program files for the signatures of known viruses, is the heart of Norton AntiVirus protection. It searches for virus signatures when you initiate manual scans, when you schedule scans to run at specific times, during startup scans that run automatically every time you start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

Manual scans



Use the Scan Now button in the Norton AntiVirus main window to initiate manual scans. These scans detect known viruses in specific files, folders, or drives on your computer. For information on how to scan files, folders, or drives, see [“Scanning for viruses”](#) on page 32.

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 40.

Startup scans



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

The startup scan is turned on during installation, unless you specifically turn it off. For information on customizing startup scans, see [“Customizing startup protection”](#) on page 95.

Auto-Protect



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

Auto-Protect is already turned on after installation, unless you specifically turn it off. For information on customizing Auto-Protect, see [“Customizing automatic protection”](#) on page 89.

Inoculation



Once your disks are scanned to verify that they are free of viruses, Norton AntiVirus inoculates boot records to make sure they stay virus-free. When a boot record is inoculated, Norton AntiVirus records critical information about it (similar to taking a fingerprint) in a special file designed specifically to store this inoculation data.

On subsequent scans, Norton AntiVirus compares the current fingerprint to its stored fingerprint. You are alerted if there are any changes that could indicate the presence of a virus. Boot records are inoculated automatically as part of your Norton AntiVirus installation. For information on inoculation, see “[Inoculating boot records](#)” on page 37 and “[Customizing inoculation](#)” on page 96.

Virus definitions files



Virus definitions files contain information that Norton AntiVirus uses during scans to detect known viruses. Norton AntiVirus depends on up-to-date information. Each time a new virus is discovered, its virus signature must be added to a virus definitions file. You should update your virus definitions files at least once per month so that Norton AntiVirus has the information it needs to find all known viruses.

New virus definitions files are available from Symantec regularly. If you have a modem or an Internet connection, Norton AntiVirus can update your virus definitions files for you automatically. See “[Automatically updating virus definitions](#)” on page 65 for information on how to receive the latest definitions.

How Norton AntiVirus warns you

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

- Virus detected during manual or scheduled scans (see Figure 1-2).
- Viruses detected by Auto-Protect (see Figure 1-3).
- Viruses detected during startup scans.

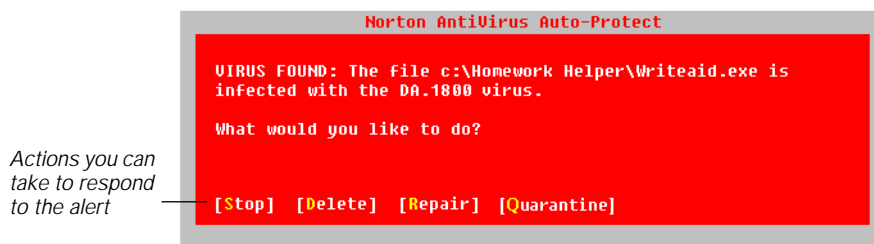
If a virus is detected during a manual or scheduled scan, the Norton AntiVirus Repair Wizard appears so you can eliminate the virus automatically. Figure 1-2 shows the opening panel of the Repair Wizard.

Figure 1-2 Norton AntiVirus Repair Wizard



Norton AntiVirus Auto-Protect, which constantly monitors for viruses, immediately displays a Virus Alert dialog box whenever an event concerning viruses occurs. (See Figure 1-3 for an example of an Auto-Protect alert.) Each Virus Alert dialog box has buttons that let you remove the virus. See “[Eliminating viruses detected during scans](#)” on page 47 for instructions on how to use the Repair Wizard.

Figure 1-3 Auto-Protect alert



Norton AntiVirus startup scans run every time you start your computer. These scans catch viruses that infect system files and boot records. Because the scans run before Windows is loaded, alerts are simply reported as text on the screen. The alert prompts you to press a key to remove the virus.

Figure 1-4 Startup scan

```
Norton AntiVirus startup scan...
Using virus definitions from
  C:\...~1\COMMON~1\SYMANT~1\VIRUSD~1\19970801.001
Using options from C:\PROGRA~1\NORTON~2
Scanning Memory... OK
Scanning Master Boot Records... OK
Scanning Boot Record... OK
C:\WIN95\WIN.COM is infected with the Cascade (1) virus.

R)epair, D)elete, C)ontinue?
```

See “[Eliminating viruses detected during startup scans](#)” on page 59 for instructions on what to do if you receive an alert during a startup scan.

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, run an infected program, or open an infected document or template.

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 89 and “Customizing startup protection” on page 95.
- Perform a manual scan (or schedule a scan to occur automatically) of your hard disks weekly. 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 32 and “Scheduling virus scans” on page 40.
- Scan all floppy disks before first use. See “Scanning for viruses” on page 32 for directions.
- Update your virus definitions files regularly. See “Automatically updating virus definitions” on page 65 for directions.
- Create and maintain a Norton AntiVirus rescue disk set to facilitate recovery from certain boot viruses. See “Creating a rescue disk set” on page 39 for directions.
- Make periodic backups of your hard disk.
- Buy legal copies of all software you use and make write-protected backups.

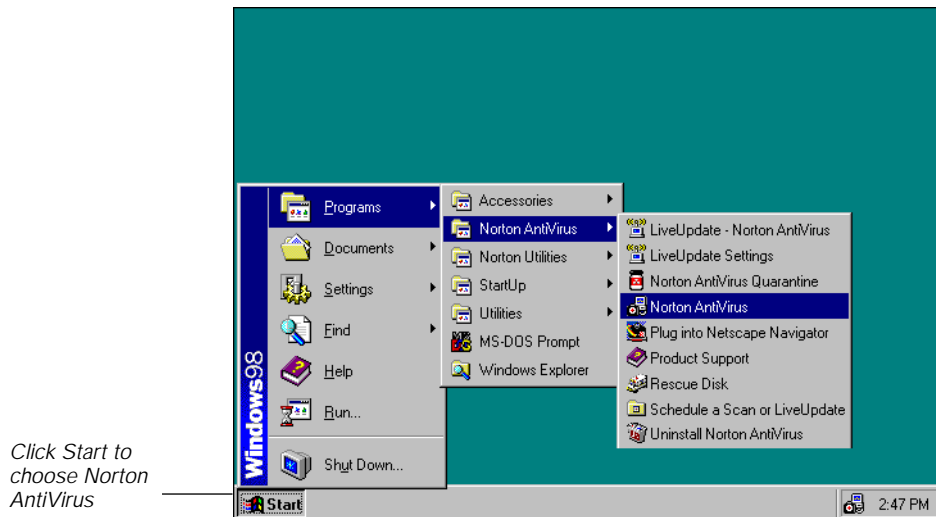
Starting and exiting Norton AntiVirus

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. Auto-Protect is always running (see “Turning Norton AntiVirus Auto-Protect off temporarily” on page 35 for information about Auto-Protect).

To start Norton AntiVirus:

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

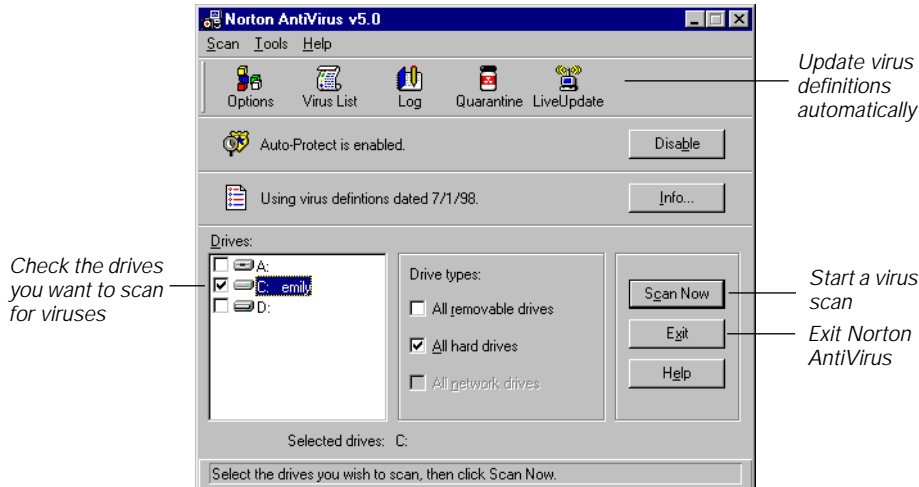
Figure 2-1 Starting Norton AntiVirus



To exit Norton AntiVirus:

- Click Exit in the Norton AntiVirus main window.

Figure 2-2 Norton AntiVirus main window



Getting help

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

To get help using Norton AntiVirus:

Do one of the following:

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

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 47). 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.

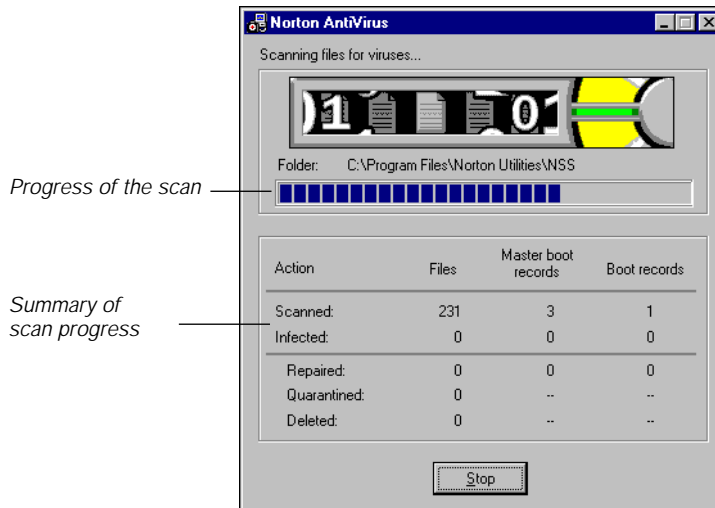
Tip: The Norton AntiVirus preset options balance maximum protection with efficiency during scans. In most cases you do not need to change anything. You can, however, customize what is scanned and what to do if a virus is found. See “[Customizing manual scan options](#)” on page 73 for directions.

To scan one or more drives:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window (see Figure 2-2), do one of the following:
 - Check specific drives to scan in the Drives list box.
 - Select multiple drives by checking items in the Drive Types group box.
- 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, choose File from the Scan menu.
- 2 Select the file you want to scan and click OK.

To scan an individual folder:

- 1 In the Norton AntiVirus main window, choose 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 program files, documents, and document templates only during a scan because these are the only types of files from which viruses spread. Occasionally, such as after a virus attack, you may

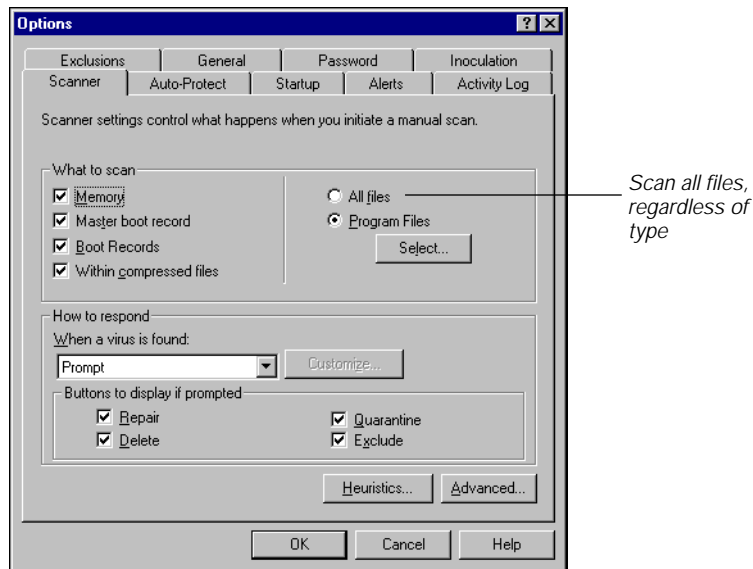
want to scan all files to make sure that a file that may not appear as a regular program file gets scanned as well.

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.

See “[Selecting which files to scan](#)” on page 78 for more information about selecting Program Files or All Files for scanning.

Figure 2-4 Scanner options tab



Turning Norton AntiVirus Auto-Protect off temporarily

Every time you start your computer, Norton AntiVirus Auto-Protect lets you know it is working. The Auto-Protect icon in the lower-right corner of the taskbar on your Windows desktop reminds you that you are fully protected against virus infection.

You are sometimes told to disable your anti-virus software when you are installing new computer programs. In this case, you disable Auto-Protect temporarily and then turn it back on again.

To turn off Norton AntiVirus Auto-Protect temporarily:



Do one of the following:

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

To turn on Norton AntiVirus Auto-Protect:



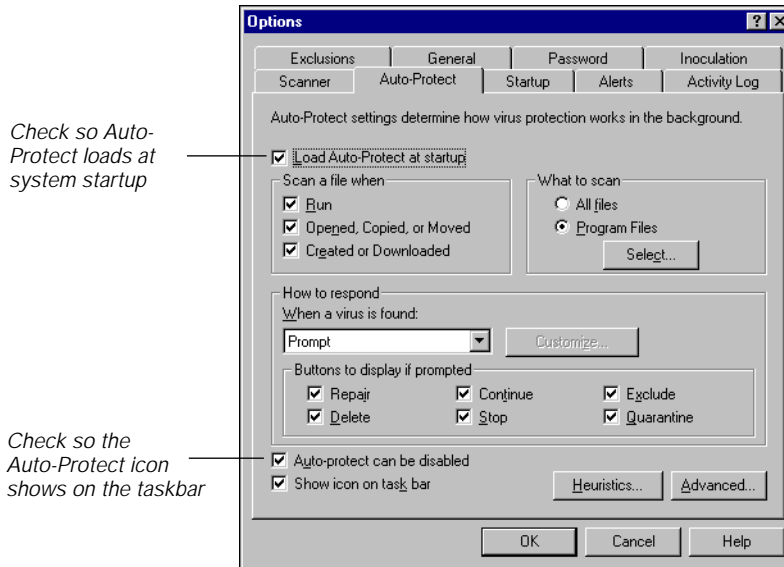
Do one of the following:

- Right-click the Norton AntiVirus Auto-Protect icon on the taskbar in the lower-right corner of your Windows desktop, then click Enable Norton AntiVirus.
- Double-click the Norton AntiVirus Auto-Protect icon on the taskbar in the lower-right corner of 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 2-5 Setting Auto-Protect options



- 4 Check Load Auto-Protect at Startup and click OK.

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

Bypassing startup protection

Startup scans, which ensure that the files your computer uses to start up are not infected, are a vital part of protecting your computer against viruses. Although it's not recommended, there may be times when you don't want Norton AntiVirus to scan for viruses during system startup. For example, you may be trying to solve a system startup problem or a configuration file conflict.

To bypass system startup scans:

- Hold down the specified bypass keys during the entire boot process. By default, they are the two Alt keys.

Bypassing system startup scans applies only to a single startup. For information on what bypass keys are, specifying what is scanned at startup, and preventing a startup scan from being bypassed, see [“Customizing startup protection”](#) on page 95.

Inoculating boot records

If you install Norton AntiVirus using the preset options, inoculation protection is set up for boot records. You don't have to do anything further.

When a boot record is inoculated, Norton AntiVirus records critical information about it (similar to taking a fingerprint) in a special data file referred to as the inoculation file. On subsequent scans—a manual scan, a scheduled scan, or an Auto-Protect scan—Norton AntiVirus checks your boot records against their stored fingerprints. You are alerted if there are any changes that could indicate the presence of an unknown virus or if a boot record is not inoculated.

Use the check box on the Options Inoculation tab to turn inoculation protection on or off for boot records. See [“Customizing inoculation”](#) on page 96 for information.

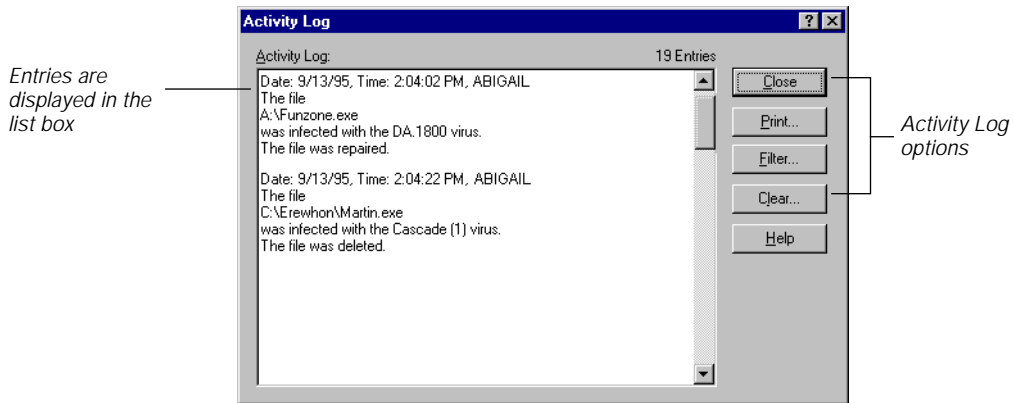
Viewing the Activity Log

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 86.

To view all entries in the Activity Log:

- 1 Click Log in the Norton AntiVirus main window.

Figure 2-6 Activity Log



- 2 Click Close to exit the Activity Log.

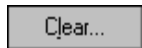
From the Activity Log dialog box you can also:



Prints 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.



Limits the display to specific types of events, such as all virus detections.

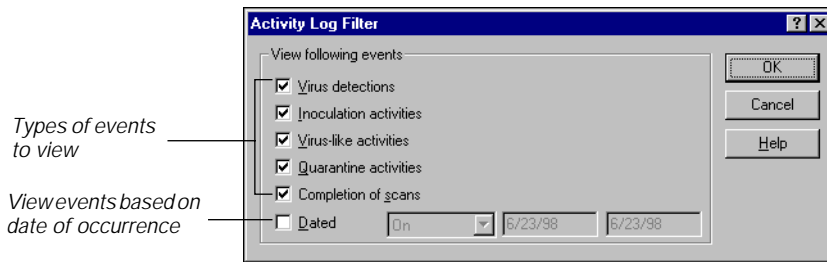


Deletes all of the entries in the Activity Log.

To filter the Activity Log entries:

- 1 Click Filter in the Activity Log dialog box (see Figure 2-6).
The Activity Log Filter dialog box appears (Figure 2-7).

Figure 2-7 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 virus detections.
 - Inoculation Activities: Displays information on boot records that have not been inoculated or have changed since inoculation.
 - Virus-like Activities: Displays information on virus-like activity detections.
 - Quarantine Activities: Displays information about items isolated in the Quarantine.
 - Completion Of Scans: Displays information about when scans occurred. This option applies to manual and scheduled scans only.

- Dated: Indicates the date or range of dates for displaying the selected events. Select an option in the Dated drop-down list box, then enter the date or dates to define the scope.
- 3 Click OK.

Creating a rescue disk set

Norton AntiVirus rescue disks protect you in case you can't start your computer or are infected by types of viruses that interfere with how files are stored on your hard disk.

Norton AntiVirus rescue disks are used to start your computer in emergencies, to detect and eliminate viruses, and to restore virus-damaged hard disks. Because the information they contain is specific to your computer, you must create them yourself.

The Rescue Disk set is composed of three separate floppy disks:

- Norton Rescue Boot Disk: Starts your computer and contains information to restore a corrupted hard disk.
- Norton AntiVirus Program Disk: Contains the Norton AntiVirus program to scan for viruses.
- Norton AntiVirus Definitions Disk: Contains the information that Norton AntiVirus uses to detect and eliminate viruses.

If you didn't create Rescue Disks during installation, create them now. You need three 1.4 MB floppy disks and three disk labels.

To create Rescue Disks:

- 1 On the Windows taskbar, click Start, point to Programs, point to Norton AntiVirus, then click Rescue Disk.

Figure 2-8 Creating a rescue disk set



- 2 Insert a floppy disk in the A: drive and click OK.
The floppy disk will be formatted as part of the process. Don't use floppy disks with files you need to keep.
- 3 Follow the prompts.
You will be notified when to change floppy disks. The entire procedure will take a few minutes.
- 4 When the Norton AntiVirus rescue disk set is created, follow the instructions on the screen to label the disks, including the computer for which they were created and the date the set was made.
- 5 Test the Norton Rescue Boot Disk to make sure it will start your computer in an emergency situation.
For directions, see ["Testing the Norton Rescue Boot Disk"](#) on page 13.

Scheduling virus scans

You can schedule virus scans that run unattended on either specific dates and times or at periodic intervals. 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. A scan is already scheduled to run automatically once per week when you install Norton AntiVirus using the preset options.

Note: Norton AntiVirus for Windows 98 and Windows 95 use different schedulers.

Scheduling scans for Windows 98

For Windows 98, Norton AntiVirus version uses the built-in Windows 98 scheduler.

To schedule a scan for Windows 98:

- 1 Click Start on the Windows taskbar, point to Programs, point to Norton AntiVirus, and click Schedule A Scan Or LiveUpdate.
- 2 In the Scheduled Tasks window, click Add Scheduled Task.
- 3 Follow the directions in the Scheduled Task Wizard.
- 4 Choose Norton AntiVirus as the application to run.

- 5 Set the scan schedule.
- 6 Close the Scheduled Tasks window.

Scheduling scans for Windows 95

For Windows 95, Norton AntiVirus uses the Norton Program Scheduler.

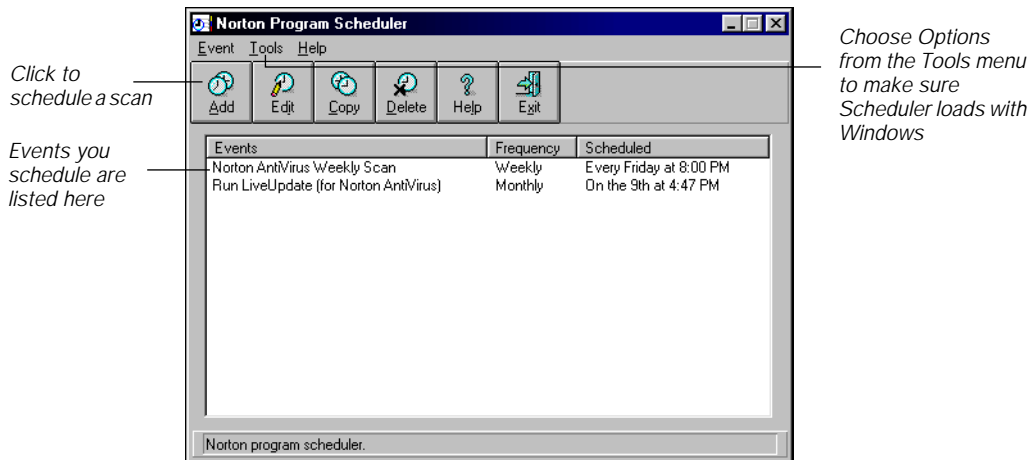
When you close the Scheduler, you can click Exit or Minimize. Make sure you click the Minimize button so that the Scheduler remains active. The Scheduler must be active before scheduled scans can run. If your computer is turned off or the Scheduler is not loaded when a scan is scheduled to take place, you are prompted to run the scan the next time the Scheduler loads.

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 2-9 The Norton Program Scheduler

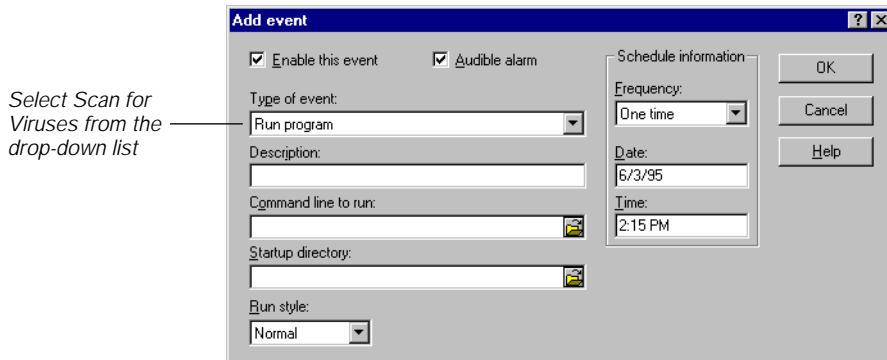


To schedule virus scans:

- 1 Click Add.

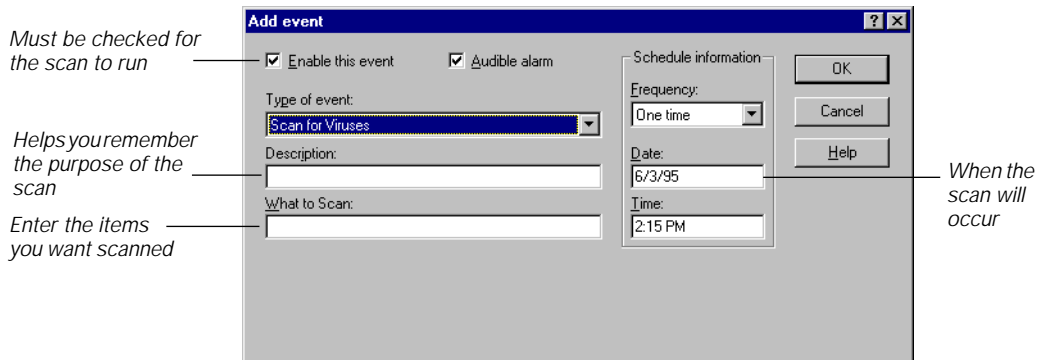
The Add Event dialog box appears so you can schedule any type of event.

Figure 2-10 Add event dialog box



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

Figure 2-11 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 "[NAVW32.EXE](#)" on page 124.

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

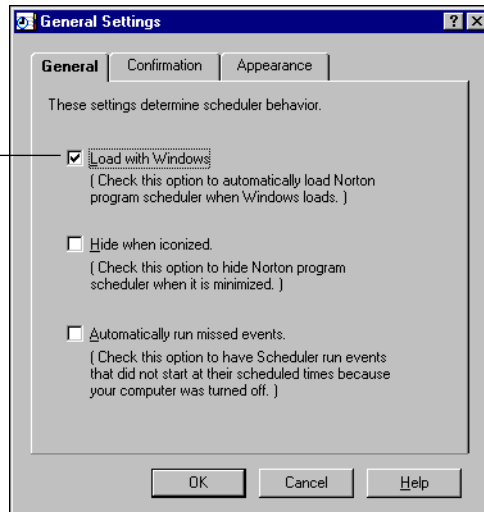
Tip: You can schedule any program to run or just display a message at a particular time. Simply select the Type Of Event in the drop-down list box and enter the requested information. The dialog box changes appropriately.

To make sure Scheduler loads when you start Windows:

- 1 Start Norton AntiVirus.
- 2 Click Scheduler in the Norton AntiVirus main window.
- 3 Choose Options from the Scheduler Tools menu.

Figure 2-12 Scheduler options settings

Make sure this is checked so that Scheduler always loads when you start Windows

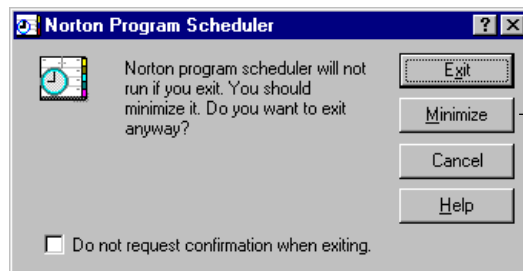


- 4 Make sure Load With Windows is checked on the General tab.
The Scheduler must be loaded in order to execute the scans you have scheduled.

To close the Scheduler:

- 1 Click Exit in the Scheduler main window.

Figure 2-13 Closing the Scheduler



Click to close the Scheduler but keep it active

- 2 Click Minimize.
The Scheduler remains active so that the scan can run at the time you specified.

To manage scheduled events:

From the Scheduler dialog box (see Figure 2-14) you can also:



Click Edit to make changes to a scheduled scan.



Click Copy to make a copy of a scheduled scan. This option is useful when you want to schedule a scan that is similar to one already on the list.



Click Delete to delete scheduled scans you no longer want.

Eliminating viruses

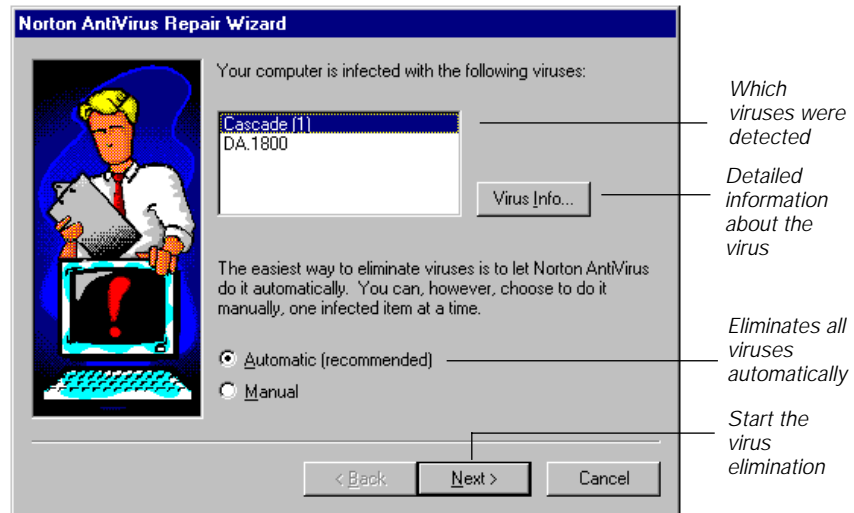
Norton AntiVirus warns you of possible virus infection in three different ways:

- Manual or scheduled scans: The Norton AntiVirus Repair Wizard appears at the end of the scan to eliminate all viruses found automatically. See “[Eliminating viruses detected during scans](#)” on page 47.
- Auto-Protect: Auto-Protect, which is constantly monitoring your computer for viruses, displays a virus alert immediately when an infected item is detected. The command buttons in the virus alert let you resolve the virus issue. See “[Eliminating viruses detected by Auto-Protect](#)” on page 53.
- Startup scans: Startup scans, which run when you first start up your computer, catch viruses that infect the files and boot records your computer uses to ready itself for work. You are prompted to press a key to eliminate the virus. See “[Eliminating viruses detected during startup scans](#)” on page 59.

Eliminating viruses detected during scans

If 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.

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 49 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



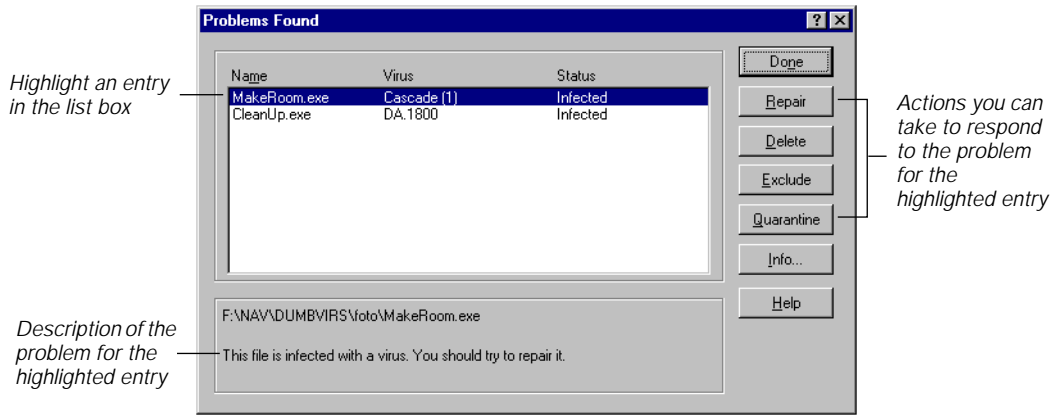
Tip: When the Repair Wizard finishes, the last panel summarizes what actions Norton AntiVirus performed. On this panel you can click More Info if you want details about the operations, or want to print a report about what was infected and repaired.

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 listing each infected item.
- 2 Highlight an entry in the list box.
- 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 See “**Command buttons**” on page 51 for information on the command buttons in the Problems Found dialog box, then click the appropriate button.

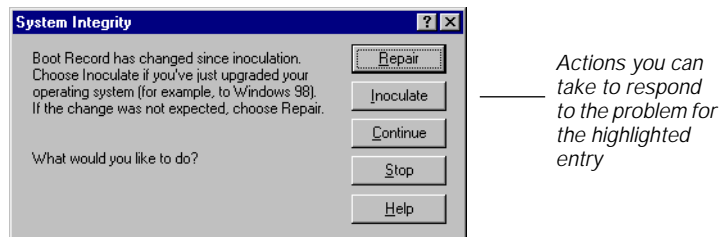
Figure 3-3 Problems Found dialog box



Responding to Inoculation alerts

Norton AntiVirus is preset to inoculate boot records the first time they are scanned. During subsequent scans, boot records are verified. Norton AntiVirus displays an Inoculation alert when a boot record has changed since it was inoculated. Changes could indicate a virus.

Figure 3-4 Inoculation alert



Inoculation changes fall into two categories:

- Expected: If you've just finished a system upgrade, the boot records may change. In this case, choose Inoculate.
For example, if you've just upgraded your computer to Windows 98 from Windows 95, this is an expected change.
- Unexpected: Changes to boot records are usually caused by viruses. If you have not recently performed an upgrade, choose Repair.

To resolve an Inoculation Change alert:



Press I (for Inoculate) if the change is expected. Inoculation makes no change to the boot record itself, the inoculation data file is merely updated.

For example, if you've just upgraded your computer to Windows 98 from Windows 95, choose Inoculate. This change is expected.



If you suspect a virus, press R (for Repair) to return the boot record to the way it was when you last inoculated it.

Warning: Choosing the wrong option for an inoculation change can corrupt your disk.



Press S (for Stop) to halt the current operation.



If you want to continue without taking any action, press C (for Continue).






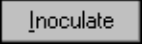

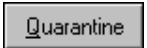
This response does not prevent Norton AntiVirus from notifying you about this file again in the future.

Command buttons

The following table explains all buttons that Norton AntiVirus may display to respond to virus issues. These buttons appear in the Problems Found dialog box, Auto-Protect virus alerts, and startup scan virus alerts. Later sections of this chapter give specific directions on how to respond to virus alerts. See “[Eliminating viruses detected by Auto-Protect](#)” on page 53 and “[Eliminating viruses detected during startup scans](#)” on page 59 for examples of virus alerts.

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, Auto-Protect, and Inoculation tabs. See [Chapter 5, “Customizing Norton AntiVirus,”](#) on page 73, for information on setting options.
- Norton AntiVirus has determined that a particular action cannot be performed in the current situation.

Button	Result	Additional Information
	Eliminates the virus and returns the infected file or boot record to its original state.	See “Responding to Auto-Protect virus found alerts” on page 56.
	For an inoculation change, returns the boot record to its previous state.	Choosing the wrong option for an inoculation change can corrupt your disk. See “Responding to Inoculation alerts” on page 50.
	Eliminates the virus by deleting the infected file.	Deleted files cannot be recovered. After the file is deleted, you must replace it with an uninfected copy.
	Stops the current operation. If a scan is in progress, the scan stops. If you are accessing a file (such as launching a program or copying a file), access is denied.	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 current operation. If a scan is in progress, it continues. If you are accessing a file (such as launching a program or copying a file), access is granted.	Selecting Continue does not solve the problem that was reported to you. If Auto-Protect generated the alert, this may allow a virus to spread.
	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 81 for more information.
	Updates stored data about the boot record that is used later to verify its integrity.	If you've just upgraded your computer to Windows 98 from Windows 95, choose Inoculate. See “Responding to Inoculation alerts” on page 50
	Displays detailed information about the virus that was found.	See “Viewing the Virus List” on page 70 for more information.
	Isolates the virus-infected file, but does not remove the virus. You can update your virus definitions and scan again.	Choose Quarantine if you suspect the infection is caused by an unknown virus. See “Submitting a file to SARC for analysis” on page 104.

Eliminating viruses detected by Auto-Protect

Norton AntiVirus Auto-Protect, which constantly monitors for viruses, immediately displays a virus alert dialog box whenever an event concerning viruses occurs. These alerts are displayed in a character-based mode because all processing, including display processing, is stopped until the possible problem is resolved.

You are warned when:

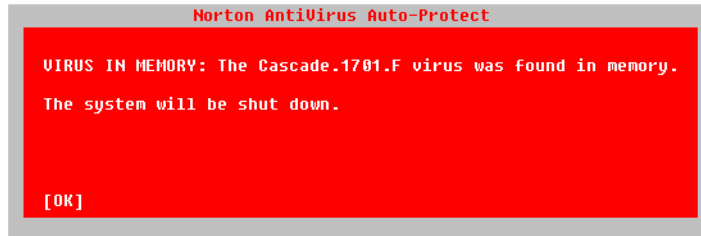
- A virus is found in a program you are trying to run or a program file you are trying to copy.
- A virus is found in memory.
- A virus-like activity is detected (an operation that viruses often perform when spreading or damaging files).

Figure 3-5 shows examples of the different types of Auto-Protect alerts.

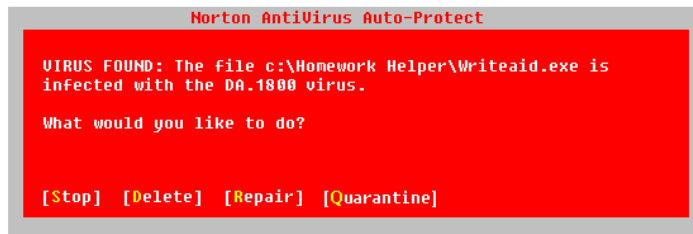
Note: For a brief description of the command buttons in virus alerts, see “[Command buttons](#)” on page 51.

Figure 3-5 Auto-Protect alerts

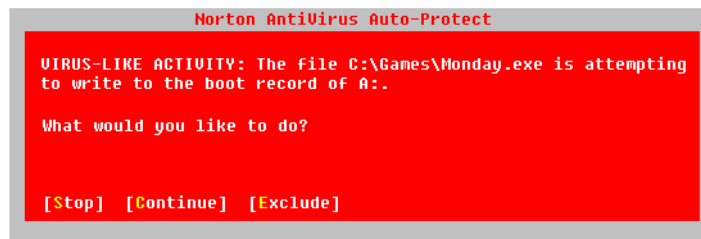
Virus in memory alert



Virus found alert



Virus-like activity alert



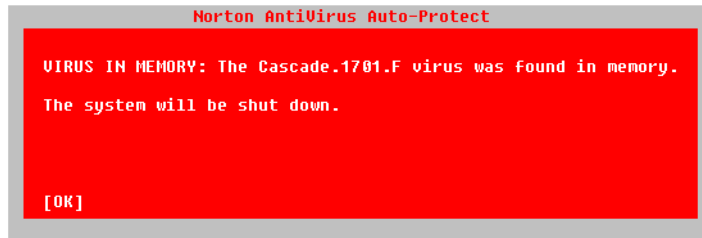
If an Auto-Protect alert appears on your screen:

- 1 Read the message in the alert box to understand the type of problem that was found.
- 2 Refer to the appropriate section for instructions on how to proceed:
 - “Responding to Auto-Protect virus in memory alerts” on page 55.
 - “Responding to Auto-Protect virus found alerts” on page 56.
 - “Responding to Auto-Protect virus-like activity alerts” on page 57.
- 3 If you see a different message that you do not understand, see Appendix D, “System messages” on page 127 for more information.

Responding to Auto-Protect virus in memory alerts

A virus in memory means the virus has been activated, is spreading to other files, and in the worst case, is damaging files on your disk. When Norton AntiVirus detects a virus in memory, all processing stops immediately.

Figure 3-6 A virus in memory alert



To respond to a virus in memory alert:

- 1 Press O for OK to shut down your computer.
- 2 Follow the Windows prompts to close applications and save data.
- 3 When the shutdown is complete, turn off your computer using the power switch.

Once you turn off your computer, the virus is removed from memory and is no longer spreading.

- 4 Use your write-protected Norton AntiVirus Rescue Disk set to restart your computer and scan again to find and remove the virus. See [“Removing viruses from a shutdown computer”](#) on page 117 for more information.

If you don't have a rescue disk set, see [“Removing viruses from a shutdown computer”](#) on page 117 for more information.

Warning: If you don't use your Norton Rescue Boot Disk or an uninfected, bootable floppy disk to restart your computer, you run the risk of activating the virus again.

Responding to Auto-Protect virus found alerts

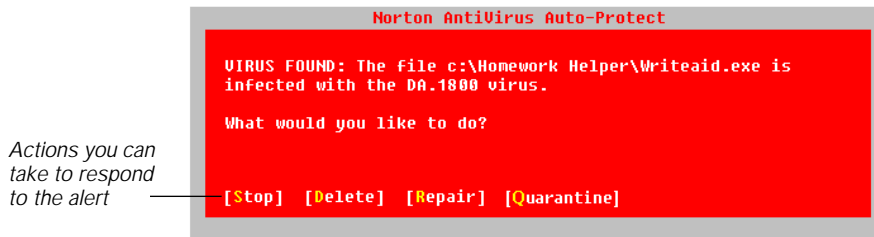
There are two ways to remove a virus from your computer:

- Repair the infected file, boot record, or master boot record.
- Quarantine the infected file.
- 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. See “What to do if repair is unsuccessful” on page 60 for instructions on how to proceed if a repair cannot be made and the file cannot be deleted.

Caution: Files deleted by Norton AntiVirus cannot be recovered even with the Norton Utilities.

Figure 3-7 A virus found alert



To repair an infected file or boot record:



- 1 Press R (for Repair) in the alert box.
If the Repair button is not displayed, either Norton AntiVirus is configured not to enable it or the item cannot be repaired.
- 2 After repairing infected files or boot records, scan your drives and floppy disks with Norton AntiVirus to verify that there aren't any other files or boot records that contain viruses.

Note: Norton AntiVirus is preset to make backup copies of files before they are repaired. Backups are stored in the Quarantine. Be sure to delete them from the Quarantine once you know the repair was successful. For more information, see “Using the Quarantine” on page 101.

Quarantine

To quarantine an infected file:

- 1 Press Q (for Quarantine) in the alert box.
- 2 After quarantining a file, open the Quarantine, update your virus definitions files, and then scan the file again.

For directions to use the Quarantine, see [“Using the Quarantine”](#) on page 101.

Sometimes Norton AntiVirus detects an unknown virus. The Symantec AntiVirus Research Center (SARC) will analyze your file to identify the virus. SARC will create and send you special updated virus definitions to detect and eliminate the new virus. For more information, see [“Submitting a file to SARC for analysis”](#) on page 104.

Delete

To delete an infected file:

- 1 Press D (for Delete) in the alert box, then follow the prompts on your screen.

If the Delete button is not displayed, either Norton AntiVirus is configured not to enable it or the item cannot be deleted.

- 2 After deleting infected files, scan all of your drives and floppy disks with Norton AntiVirus to verify that there aren't any other files that contain viruses.
- 3 Once you are certain that your system is virus-free, replace the files you deleted with uninfected copies.

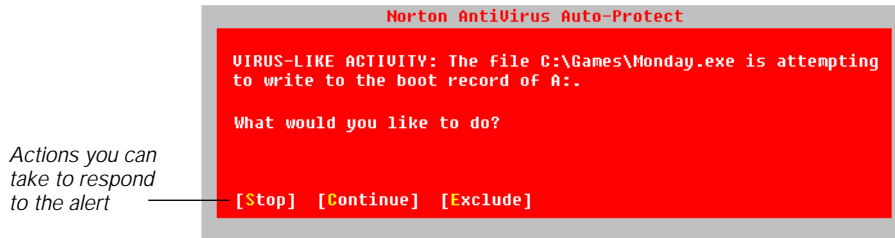
Make sure you scan the replacement files before copying them to your hard disk.

Tip: 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 37.

Responding to Auto-Protect virus-like activity alerts

A virus-like activity alert appears when Norton AntiVirus detects an activity that viruses often perform when spreading or doing damage to your files. These alerts are displayed in a character-based mode rather than in graphical mode. Norton AntiVirus stops all processing, including display processing, until the virus-like activity alert is resolved.

Figure 3-8 Virus-like activity alert



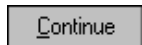
NOTE: A virus-like activity alert does not necessarily mean your computer has a virus—it is simply a warning. It's up to you to decide whether the operation is valid in the context in which it occurred. For a description of each virus-like activity that Norton AntiVirus detects, see [“Customizing automatic protection”](#) on page 89.

To resolve an Auto-Protect virus-like activity alert:



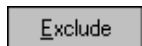
If the activity detected is not related to what you are trying to do, press S (for Stop) to prevent the action from taking place.

For example, if you are playing a game and receive an alert stating that there is an attempt to write to the boot records of your hard disk, select Stop to prevent your disk from being modified.



If the message in the alert box describes an activity that is valid in the context of the application you are running, press C (for Continue) to allow the activity to proceed.

For example, if you are updating a software program and the alert warns you that there is an attempt to write to a program file, select Continue.



If the activity is valid in the context of the application you are running and you don't want Norton AntiVirus to alert you of this activity (performed by this application) in the future, press E (for Exclude).

For example, if you are using a disk format utility to create a bootable floppy disk, you may want to select Exclude to prevent Norton AntiVirus from warning you every time you use the program to format a floppy disk.

Eliminating viruses detected during startup scans

Norton AntiVirus startup scans catch viruses that infect the files and boot records your computer uses to ready itself for work. They are a vital part of virus protection because they make sure that your computer is virus-free each time you start it up. Viruses found during startup scans are a serious issue and must be resolved immediately: all files and data are at risk.

You are warned when:

- A virus is found in memory.
- A virus is found in a system program or boot record.

Because startup scans are run before Windows loads, alerts are displayed as text messages on the screen. You are prompted to press a key to resolve the problem.

Responding to startup scan virus in memory alerts

A virus in memory means the virus has been activated, is spreading to other files, and in the worst cases, is damaging files on your disk. When Norton AntiVirus detects a virus in memory, all processing stops immediately.

Figure 3-9 Startup scan virus in memory alert

```
Norton AntiVirus startup scan...
Using virus definitions from
  C:\...~1\COMMON~1\SYMAN~1\VIRUSD~1\19970801.001
Using options from C:\PROGRA~1\NORTON~2

Scanning Memory...
The DarkAvenger.Main.HLT virus was found in memory.
Restart your computer from your Norton AntiVirus Emergency
  Boot Disk and follow the onscreen instructions.
```

To respond to a startup scan virus in memory alert:

- 1 Turn off your computer using the power switch.
Once you turn off your computer, the virus is removed from memory and is no longer spreading.
- 2 Use your write-protected Norton Rescue Boot Disk to restart your computer and scan again to find and remove the virus. See

“[Removing viruses from a shutdown computer](#)” on page 117 for more information.

Responding to startup scan virus found alerts

Virus found alerts on startup scans are a serious issue. A virus in a system file or boot record means your whole computer is at immediate risk. You should let Norton AntiVirus repair the infected item to eliminate the virus.

Figure 3-10 Startup scan virus found alert

```
Norton AntiVirus startup scan...
Using virus definitions from
  C:\...~1\COMMON~1\SYMANT~1\VIRUSD~1\19970801.001
Using options from C:\PROGRA~1\NORTON~2

Scanning Memory... OK
Scanning Master Boot Records... OK
Scanning Boot Record... OK
C:\WIN95\WIN.COM is infected with the Cascade (1) virus.
R)epair, D)elete, C)ontinue?
```

To repair a startup scan infected file or boot record:

- 1 Press R (for Repair).
- 2 After repairing infected files or boot records, scan your drives and floppy disks again with Norton AntiVirus.

This verifies that there aren't any other files or boot records that contain viruses.

You cannot delete infected boot records, master boot records, and some system files to remove a virus because they contain information your computer uses to start up. See “[What to do if repair is unsuccessful](#)” on page 60 for instructions on how to proceed if a repair cannot be made and the item cannot be deleted.

What to do if repair is unsuccessful

One of the most common reasons Norton AntiVirus can't repair a file is that you don't have the most up-to-date virus protection files. Click LiveUpdate in the Norton AntiVirus main window to obtain the latest files via modem or Internet.

Do one of the following:

- Update your virus protection and scan again. See “[Automatically updating virus definitions](#)” on page 65 for details.
- Read the information on your screen carefully to identify the type of item that can't be repaired, then match it to one of the types below:
 - Infected files are those with filenames that include .COM or .EXE. Document files such as .DOC, .DOT, and .XLS can also be infected.
 - Compressed files may contain many files. You can often tell a compressed file by its name. Many compressed files end in .ZIP.
 - Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files are replaced using the Rescue Disks or, sometimes, your operating system (Windows or DOS) disks.

Infected files

If infected files can't be repaired, you need to either quarantine or delete them from your computer. If you leave an infected file on your computer, the virus infection can still spread.

If Norton AntiVirus can't repair a file:

Do one of the following:

- Choose Quarantine.

After the file is quarantined, you can update your virus definitions and scan again or submit the file to SARC for analysis. For more information, see “[Using the Quarantine](#)” on page 101 and “[Submitting a file to SARC for analysis](#)” on page 104.
- Choose Delete.

Replace the deleted document file with a backup copy or reinstall a deleted program from the original program disks. Make sure to scan the backup disks before you use them.

If the virus is detected again after you replace or reinstall the file, your backup copy or original program disks are probably infected. You can try contacting the manufacturer for a replacement.

Compressed files

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 uncompress (open up) the compressed file.

To uncompress and repair:

- 1 Double-click the Norton AntiVirus Auto-Protect icon in the lower-right corner of the taskbar on your Windows desktop.
- 2 Click Disable to turn Auto-Protect off temporarily.
- 3 Create a temporary folder (for example, C:\TEMP).
- 4 Move the infected, compressed file to the temporary folder.
- 5 Use a program such as Norton Navigator, WinZip, or PKUNZIP to uncompress the file in the temporary folder.
- 6 On the Windows taskbar, click Start, point to Programs, point to the Norton AntiVirus group, then click Norton AntiVirus.
- 7 From the Scan menu at the top of the Norton AntiVirus main window, choose FOLDERS.
- 8 Select the C:\TEMP folder, then click Scan to scan the files again.
- 9 Let the Repair Wizard automatically repair all the infected files.
- 10 Click Exit to close Norton AntiVirus.
- 11 Delete the infected, compressed file.
- 12 Recompress the files, if desired.
- 13 Double-click the Norton AntiVirus Auto-Protect icon in the lower-right corner of the taskbar on your Windows desktop.
- 14 Click the Enable button to turn Auto-Protect on again.

Hard disk master boot record or boot record

Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files are replaced using the Rescue Disks or, sometimes, your operating system (Windows or DOS) disks.

If Norton AntiVirus can't repair your hard disk or master boot record, you can use your up-to-date Norton Rescue Boot Disk to restore it. See ["Restoring your hard disk"](#) on page 118 for details.

Floppy disk boot record

If Norton AntiVirus cannot repair a floppy disk boot record, it still removes the virus. The information on the floppy disk remains accessible and you can safely copy the files onto another disk. However, the floppy disk is no longer bootable.

System file

If Norton AntiVirus cannot repair a system file (for example, IO.SYS or MSDOS.SYS) you cannot delete it. You must reinstall Windows.

Restart your computer from an uninfected, write-protected floppy disk and reinstall Windows. You can use your Norton Rescue Boot Disk or the Windows 95/98 Startup Disk that you created when you installed Windows to start up.

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, you should update your virus definitions files at least monthly.

Automatically updating virus definitions

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

- Internet connection
- Properly connected modem

Make it a practice to update your virus definitions once every month.

Figure 4-1 Update virus definitions automatically

Specify how to connect or let Norton AntiVirus choose automatically



To update virus definitions automatically:

- 1 In the Norton AntiVirus main window, click LiveUpdate (see Figure 4-1).
- 2 In the How Do You Want To Connect drop-down list box, select one of the following:
 - Find Device Automatically: Norton AntiVirus determines if you have an Internet connection or must connect using your modem.
 - Internet: Norton AntiVirus connects to the Symantec FTP (File Transfer Protocol) site on the Internet.
 - Modem: Norton AntiVirus dials a preset number and connects to a Symantec server through your modem.

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

- 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.

Tip: After a LiveUpdate, read the new text documents (*.TXT) that are downloaded to your definitions folder for late-breaking information about newly discovered viruses and any special precautions that you should take. By default, the definitions folder is C:\Program Files\Common Files\Symantec Shared\VirusDefs\nnnnnnnnn.nnn. The last folder (nnnnnnnnn.nnn) represents a date. Select the one with the most recent Modified date.

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 From your web browser, go to <http://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 in Windows 98

For Windows 98, Norton AntiVirus uses the new built-in Windows 98 scheduler.

To schedule automatic LiveUpdates for Windows 98:

- 1 Click Start on the Windows taskbar, point to Programs, point to Norton AntiVirus, and click Schedule A Scan Or LiveUpdate.
- 2 In the Scheduled Tasks window, click Add Scheduled Task.
- 3 Follow the directions in the Scheduled Task Wizard.
- 4 Choose LiveUpdate as the application to run.
- 5 Set the LiveUpdate schedule.
- 6 Close the Scheduled Tasks window.

Scheduling an automatic LiveUpdate in Windows 95

For more information about using the Norton Program Scheduler, see [“Scheduling virus scans”](#) on page 40.

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.

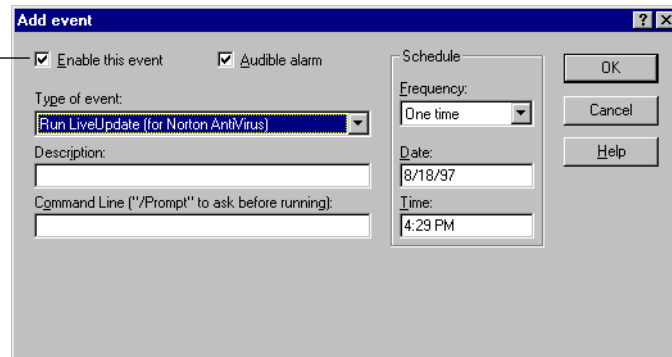
The Add Event dialog box appears.

- 3 Select Scheduled LiveUpdate in the Type Of Event drop-down list box.

The dialog box changes to accept information specific to LiveUpdate.

Figure 4-2 Add event dialog box for 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 box.
- 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 the Symantec website (<http://www.symantec.com>) and other sources listed in the Service and Support Solutions in this guide.

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 Explorer window, double click the Intelligent Updater program.
- 3 Follow all prompts displayed by the update program.
- 4 The update program will install the new virus definitions files in the proper folder automatically.
- 5 Initiate a scan with Norton AntiVirus to activate the new virus definitions.
- 6 Restart your computer so that Auto-Protect uses the virus definitions files as well.

Tip: After a LiveUpdate, read the new text documents (*.TXT) that are downloaded to your definitions folder for late-breaking information about newly discovered viruses and any special precautions that you should take. By default, the definitions folder is C:\Program Files\Common Files\Symantec Shared\VirusDefs\nnnnnnnnn.nnn. The last folder (nnnnnnnnn.nnn) represents a date. Select the one with the most recent Modified date.

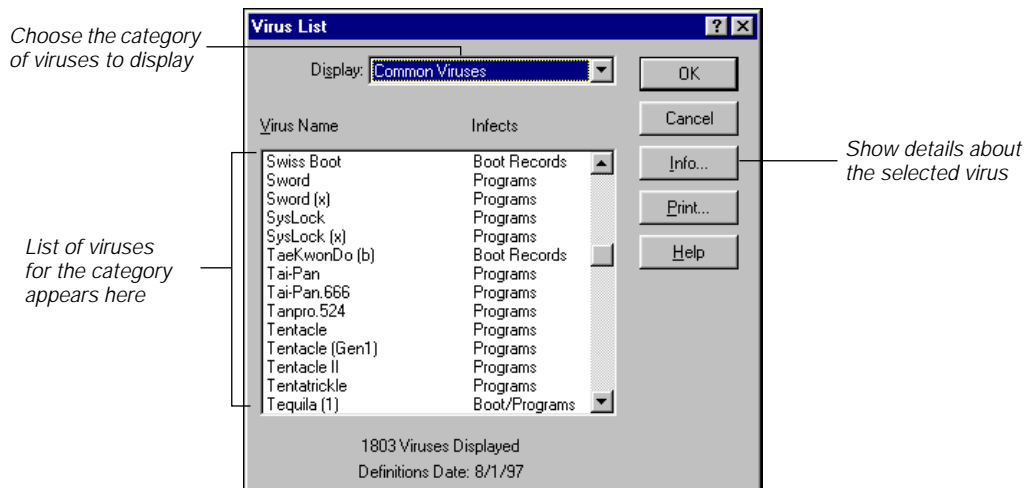
Viewing the Virus List

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 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.
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 box by clicking inside the list box (see Figure 4-3).

- 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

Norton AntiVirus is a powerful weapon in the war against viruses. The preset options from your Norton AntiVirus installation are designed to provide excellent protection for all computing environments. Unless you are a computer professional with special implementation requirements, it is unlikely that you will want or need to modify your Norton AntiVirus configuration. When you install Norton AntiVirus and accept the preset options, you are protected. You don't have to change anything.

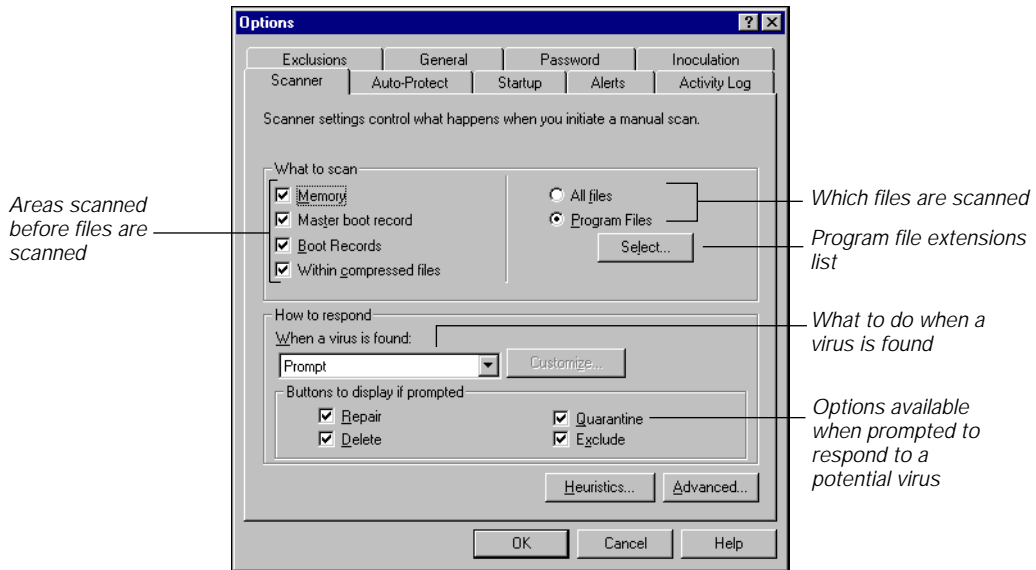
Customizing manual scan options

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.

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:

- Memory: Checks for viruses resident in your computer's memory.

It is important to check this option because viruses resident in memory are actively spreading to other files. If this option is left unchecked, a memory-resident virus can spread to every file scanned.

- 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 any one of several popular compression utilities. Compressed files within compressed files are not scanned. Scanning time may increase slightly if you have many compressed files.

- 4 Also specify in the What To Scan group box 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 78.

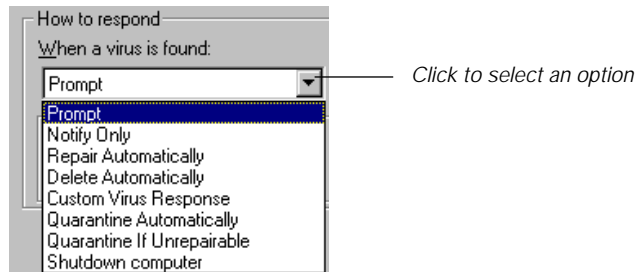
Note: The extensions for Microsoft Word documents and Microsoft Excel spreadsheets are included in the program files group. Although these are not program files, they can be infected by the class of viruses called macro viruses.

- 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 5-2).
- 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: Merely informs you when a virus is detected. You will not be able to repair or delete 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 general scanning options](#)” on page 88.
- **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 Virus 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 so that it cannot spread, but does not attempt a repair.
- **Quarantine If Unrepairable:** Isolates a virus-infected file that cannot be repaired. From the Quarantine you can submit the file to the Symantec AntiVirus Research Center (SARC) for analysis. See “[Submitting a file to SARC for analysis](#)” on page 104.
- **Shutdown Computer:** Shuts down your computer when a virus is detected.

To remove a virus after shutdown, insert your Norton Rescue Boot Disk (the first disk of your Norton AntiVirus rescue disk set) and restart your computer. Scan again to find and remove the virus. See “[Removing viruses from a shutdown computer](#)” on page 117 for directions.

Caution: Shutdown Computer instructs Norton AntiVirus to quit all applications and shut down immediately. You won’t have an opportunity to save your work.

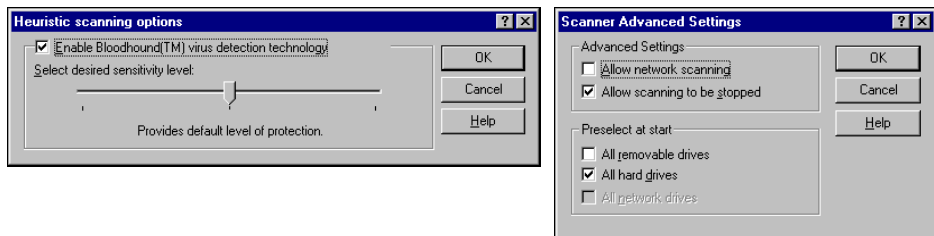
- 4 If you selected Prompt in step 3, specify in the Buttons To Display If Prompted group box which options you want Norton AntiVirus to make available when a virus is found:
 - **Repair:** Allows you to repair the file or boot record. If the virus infects an item that cannot be repaired, such as an in-use file, the button will be dimmed.

- Delete: Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button will be dimmed.
 - Quarantine: Isolates the virus-infected file so that it cannot spread, but does not attempt a repair. From the Quarantine you can submit the file to the Symantec AntiVirus Research Center (SARC) for analysis. See [“Submitting a file to SARC for analysis”](#) on page 104.
 - Exclude: Allows you to 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).
- 2 Make sure that Enable Bloodhound Virus Detection Technology is checked.
Norton AntiVirus includes a new technology called Bloodhound to dramatically increase your virus protection against difficult to detect and unknown 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.

Figure 5-3 Additional Scanner settings



- 5 Click the Advanced button in the Scanner tab (see Figure 5-2).
The Scanner Advanced Settings dialog appears (see Figure 5-3).

- 6 Check the Advanced Settings options that you want to enable:
 - Allow Network Scanning: Lets you scan network drives. See “Notes on scanning network drives” on page 78 for network scanning restrictions.
 - 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.
- 7 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.
- 8 Click OK to save your settings and close the dialog box.

Notes on 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 or delete infected files, or inoculate
Read-Write	Scan, repair, delete, and inoculate

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

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 or Microsoft Word documents 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

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 Microsoft 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. See [“Customizing manual scan options”](#) on page 73 and [“Customizing automatic protection”](#) on page 89 for information on setting these options.

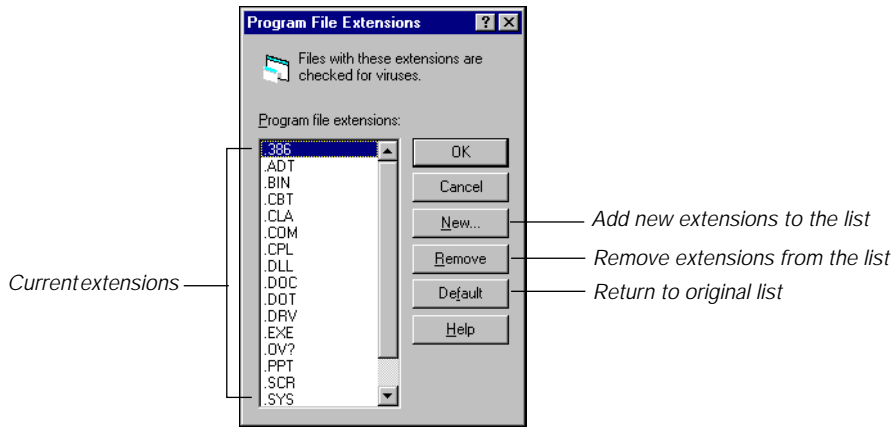
Specifying program file extensions

Norton AntiVirus uses the program file extensions list when scanning and inoculating program files. 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

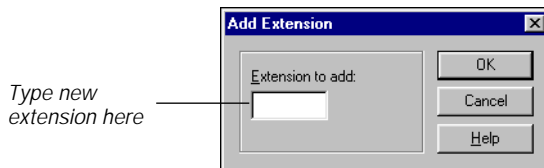


The file extensions list contains the majority of program file extensions. If you use custom applications that use unique file extensions, add them to the list.

To add a program file extension:

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

Figure 5-5 New Program File Extension dialog box



- 2 Type the new file extension in the Extension To Add text box and click OK.

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.)

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 and click OK.

To reset the list of program file extensions:

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

The list of extensions returns to the way it was when you installed Norton AntiVirus.

- 2 Click OK.

Managing exclusions

Norton AntiVirus refers to the entries in the exclusions list during all scans it performs. An exclusion is a condition or virus-like activity that would normally be detected, but you have told Norton AntiVirus not to check for a particular file. An exclusion applies to a specific filename. If you move or rename a file, its exclusion doesn't move with it. You automatically invalidate the exclusion.

For example, because the operating system program FORMAT legitimately writes to the boot record of a floppy disk, you may want to exclude that activity for FORMAT.COM. By adding this activity to the exclusions list, you are telling Norton AntiVirus to ignore all writes to floppy disk boot records performed by FORMAT. But the file will still be checked for known viruses when scanned.

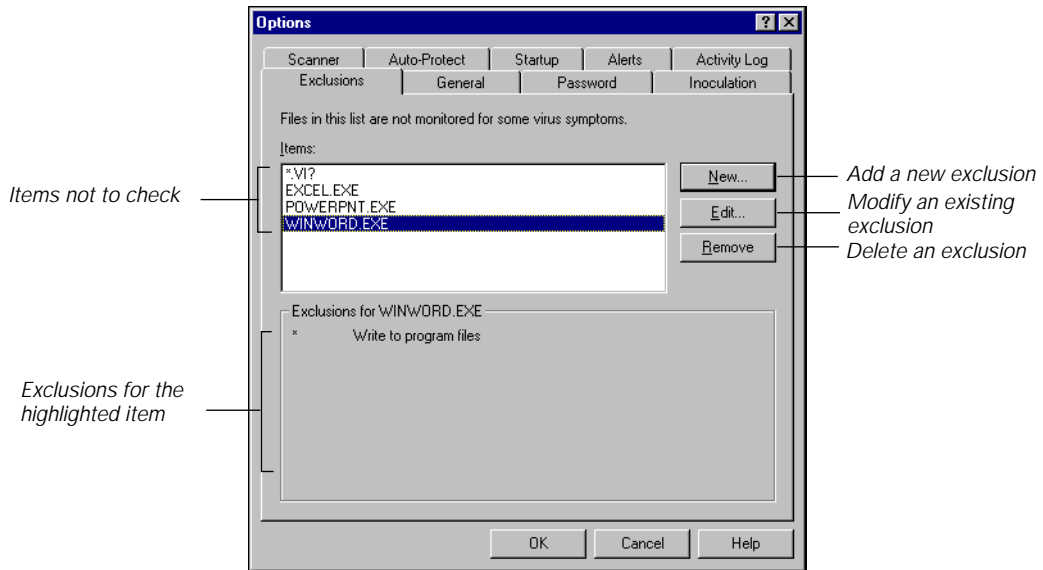
Excluding files doesn't mean "don't find viruses" (unless you specifically select that option); rather, it means "let some activity proceed" because you know a virus did not cause it. Be careful. If you set an exclusion, a virus can creep in.

Note: By default, the Microsoft Office executables are excluded for Write To Program Files. This prevents an Auto-Protect alert from being generated every time a .DOC or .XLS file is saved. The Office executables, however, are still scanned for viruses.

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



3 Select a file or group of files in the Items list box.

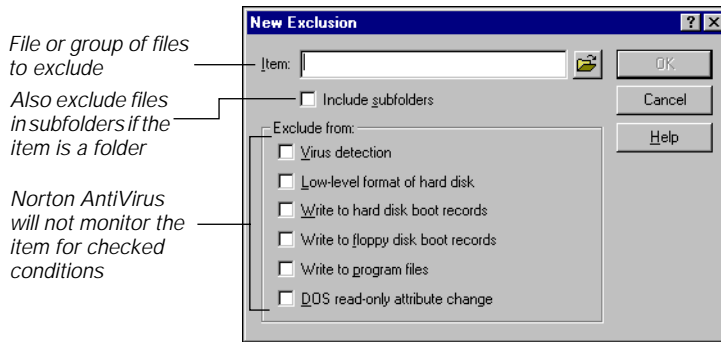
The activities excluded for the file or files are displayed in the Exclusions For group box.

In most cases, items are added to the exclusions list when you click Exclude in an alert to resolve a virus detection event that you deem acceptable. Although you can add exclusions to Norton AntiVirus manually, it is not a good idea unless you are sure of what you are doing.

To add exclusions manually:

- 1 Click New in the Exclusions tab (see Figure 5-7).

Figure 5-7 Adding a new exclusion



- 2 Type the pathname for the file or group of files in the Item text box.
- 3 Check Include Subfolders if you want to exclude files in descending folders also.
- 4 Check the activities that you want Norton AntiVirus to exclude from detection:
 - Virus Detection: Exclude the item from checks for known viruses.
 - Low-level Format Of Hard Disk: Exclude the item from checks for attempts to perform a low-level format of your hard disk, which obliterates all information on the disk.
 - Write To Hard Disk Boot Records: Exclude the item from checks for attempts to write to the boot records on your hard disk. This action is performed legitimately by very few programs.
 - Write To Floppy Disk Boot Records: Exclude the item from checks for attempts to write to the boot record on a floppy disk. This action is performed legitimately by very few programs.
 - Write To Program Files: Exclude the item from checks for attempts to write to a program file. Some programs save configuration information within themselves rather than in a separate file.
 - DOS Read-Only Attribute Change: Exclude the item from checks for attempts to change a read-only file so that it can be written to. This option applies specifically to operations executed by DOS applications.

Note: Although excluding files from specific checks can be useful, be cautious when excluding files because it can also reduce your virus protection.

- 5 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.

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 and click OK.

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

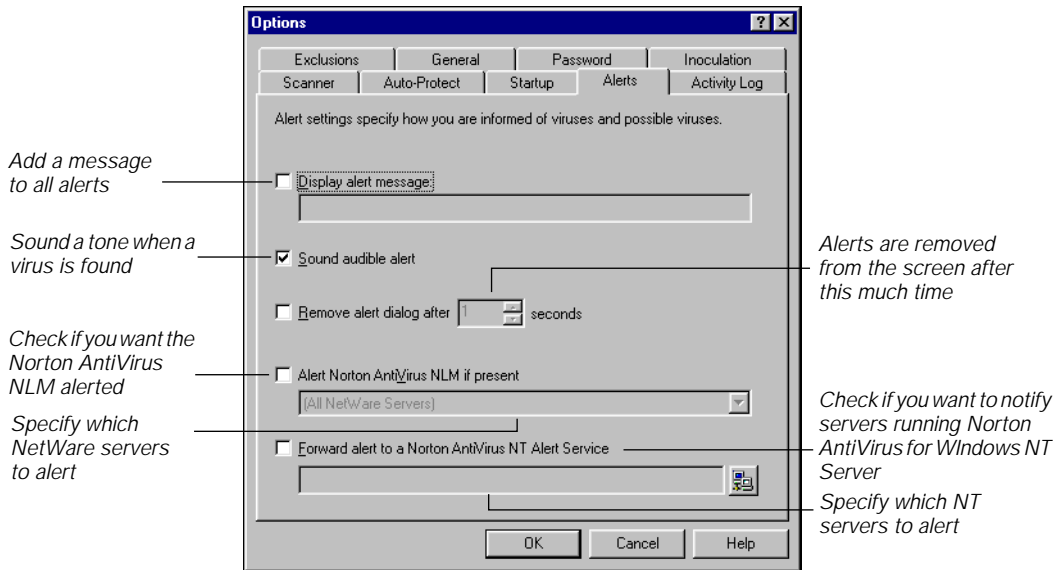
Customizing alerts

The alert settings define how Norton AntiVirus informs you that it has detected a virus or possible virus. These options apply to all scans that Norton AntiVirus performs (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.

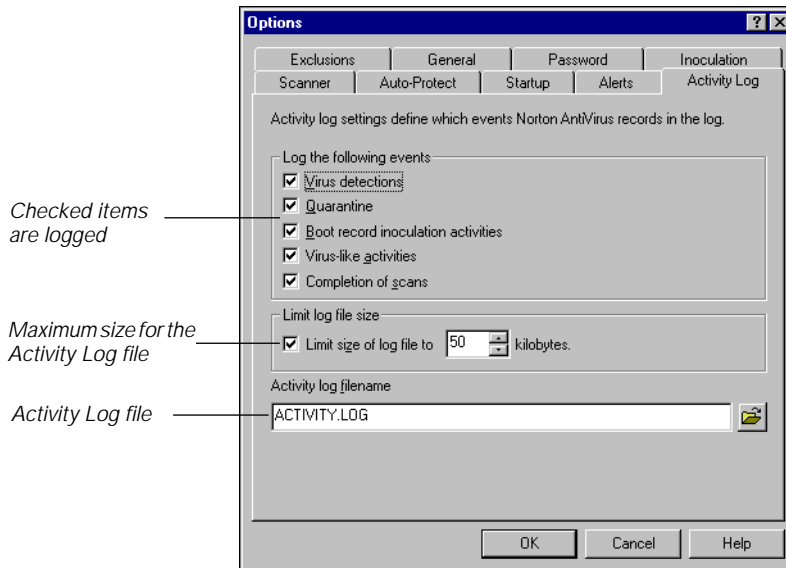
Customizing the Activity Log

The Activity Log contains a history of Norton AntiVirus activity. For example, Norton AntiVirus is preset to record detections of known viruses and the action performed on infected files (whether they were repaired, deleted, added to the exclusions list, or left untouched). You can customize the Activity Log to record other types of events (such as unknown virus detections and Virus List changes) as well.

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



- 3 In the Log Following Events group box, check each type of event that you want Norton AntiVirus to record:
 - Virus Detections: Records detections of all viruses.
 - Quarantine: Records all items sent to the Quarantine.
 - Boot Record Inoculation Activities: Records detections of uninoculated and changed boot records.
 - Virus-like Activities: Records detections of virus-like activities (activities that many viruses perform when spreading or damaging data, such as an attempt to format your hard disk).
 - Completion Of Scans: Records the date and ending time of scans that you initiate and scheduled scans.
- 4 If you want to limit the Activity Log file to a particular size, check Limit Size Of Log File To, then enter the maximum size in the Kilobytes text box.
 When the Activity Log reaches the specified size, each new entry added to the activity log replaces the oldest entry or entries.
- 5 Enter the pathname for the Activity Log file in the Activity Log Filename text box.
- 6 Click OK to save settings and close the dialog box.

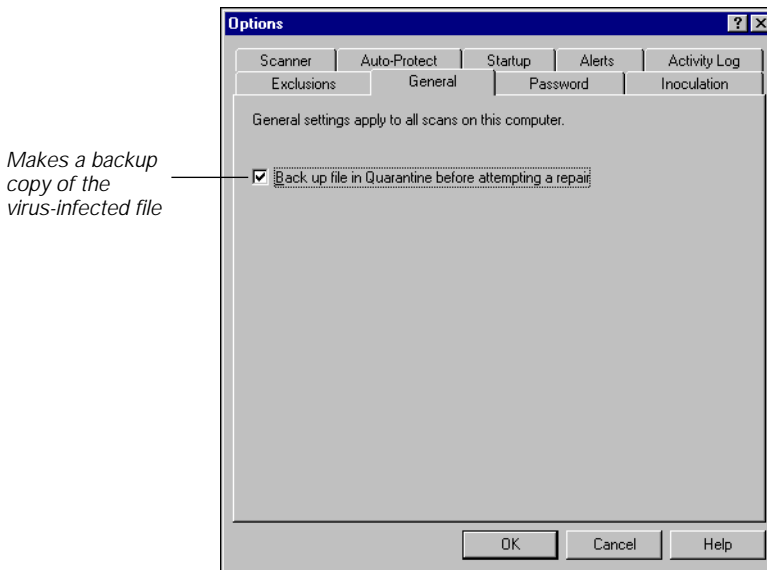
Setting general scanning options

The general scanning options apply to all scans—scans you initiate, scheduled scans, and scans performed by Auto-Protect.

To customize general scanning options:

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

Figure 5-10 General settings



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

Note: Delete these backup files from the Quarantine after you determine that the repair operation is successful. Even though the infected backup files can't be run, they contain viruses. See [“Managing the Quarantine,”](#) on page 101 for more information.

- 4 Click OK.

Customizing automatic protection

The automatic protection feature protects your computer against viruses by:

- Checking programs for viruses when you run them and floppy disks for viruses when you access them.
- Monitoring your computer for signs of unknown viruses or virus-like activities.
- Preventing 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 73.

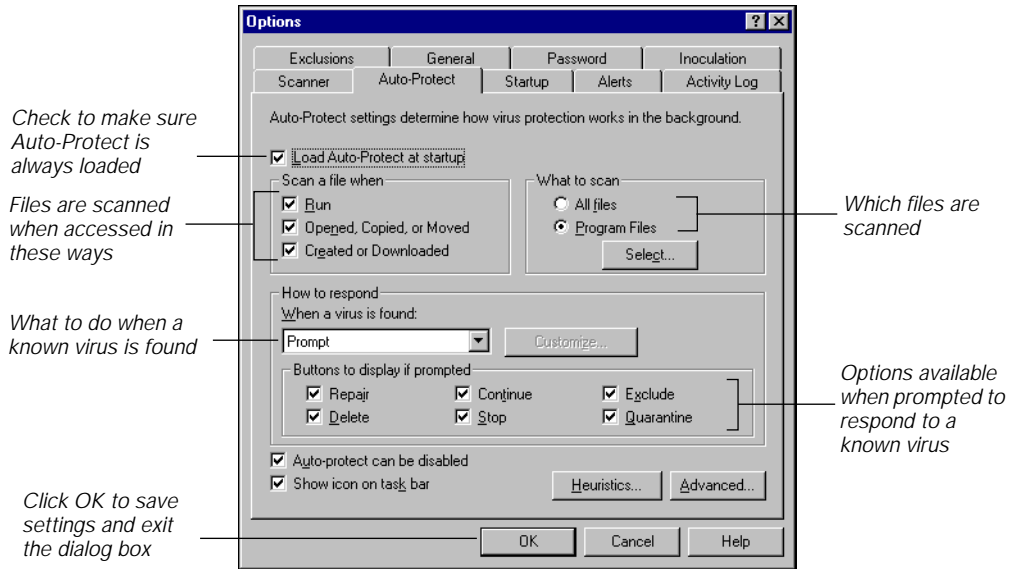
Auto-Protecting program files

Norton AntiVirus can check for viruses whenever you open a file or run a program.

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.

Note: 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:
 - Run: Scans a program file each time you run it.
 - Opened, Copied, or Moved: Scans files when they are opened. For example, when you copy a file, Norton AntiVirus scans the file you are copying.
 - Created or Downloaded: Scans files when they are created on your drive by an installation program, by decompressing files, or by downloading files from a bulletin board system.
- 5 Select an option in the What To Scan group box:
 - All Files: Scans all files that you access, includes files less likely to contain 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 78.

- 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:
 - **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.
 - **Deny Access:** Prevents the file from being opened.
 - **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 general scanning options”](#) on page 88.
 - **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.
 - **Shutdown Computer:** Shuts down your computer when a virus is detected. See [“Removing viruses from a shutdown computer”](#) on page 117.
 - **Quarantine Automatically:** Isolates the virus-infected file so that it cannot spread, but does not attempt a repair.
 - **Quarantine If Unrepairable:** Attempts a repair, but isolates a virus-infected file that cannot be repaired. From the Quarantine you can submit the file to the Symantec AntiVirus Research Center (SARC) for analysis. See [“Submitting a file to SARC for analysis”](#) on page 104.

Caution: Shutdown Computer instructs Norton AntiVirus to quit all applications and shut down immediately. You will not have an opportunity to save your work, but it will stop a virus from spreading.

- 4 If you selected Prompt in step 3, specify in the Buttons To Display If Prompted group box which options to make available when a known virus is found:
 - Repair: Allows you to repair the file or boot record. If the virus infects an item that cannot be repaired, such as an in-use file, the button will be dimmed.
 - Delete: Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button is not displayed.
 - Continue: Allows you to continue accessing the file. If you select the Continue button, you may activate the virus.
 - Stop: Allows you to stop the file access. The virus will not be activated, but the file is still infected.
 - Exclude: Allows you to exclude the file from future checks for known viruses. Use caution when using this button; it reduces your protection against viruses.
 - Quarantine: Isolates the virus-infected file so that it cannot spread, but does not attempt a repair. From the Quarantine you can submit the file to the Symantec AntiVirus Research Center (SARC) for analysis. See [“Submitting a file to SARC for analysis”](#) on page 104.
- 5 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.
- 6 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.
- 7 Click OK to save your settings and close the dialog box or continue to the next procedure.

Monitoring for virus-like activities

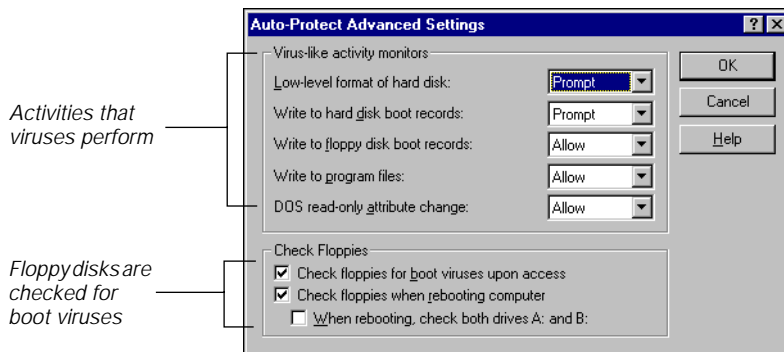
A virus-like activity is an action that viruses typically perform when damaging your files or spreading through your system. Although some

applications perform these actions for valid reasons, Norton AntiVirus can monitor for the activities to prevent them from being performed by an unknown virus.

To monitor for virus-like activities:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Auto-Protect tab.
- 3 Click Advanced in the Auto-Protect tab (see Figure 5-11).

Figure 5-12 Auto-Protect Advanced Settings



- 4 Select a monitoring option in each drop-down list box to specify what Norton AntiVirus should do when it detects the virus-like activity:
 - Allow: Allows the activity to continue every time without informing you. Selecting Allow offers you no protection against an unknown virus performing the activity.
 - Prompt: Informs you when a program tries to perform the activity and allows you to decide whether to Continue, Stop, or Exclude. Although excluding files from specific checks can be useful, be careful. Excluding files can reduce your virus protection.
 - Don't Allow: Prevents the activity from occurring every time it is detected.

The virus-like activities include:

- Low-level Format Of Hard Disk: All information on the disk is erased and cannot be recovered. This type of format is generally performed by the manufacturer. If this activity is

detected, it almost certainly indicates an unknown virus at work.

- Write To Hard Disk Boot Records: Very few programs write to hard disk boot records. Unless you are specifically using a program that writes to the hard disk boot records, such as FORMAT, this activity probably indicates a virus.
 - Write To Floppy Disk Boot Records: Only a few programs (such as the operating system FORMAT or SYS commands) write to floppy disk boot records.
 - Write To Program Files: Some programs save configuration information within themselves. Although this activity often happens legitimately, it could indicate an unknown virus at work.
 - DOS Read-Only Attribute Change: Many programs change a file's read-only attribute. Although this activity often happens legitimately, it could indicate an unknown virus at work. This option applies specifically to operations executed by DOS applications.
- 5 Click OK to close the dialog box.
 - 6 Click OK to save your settings and close the Options 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 Click Advanced in the Auto-Protect tab.
- 4 In the Check Floppies group box (see Figure 5-14), 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.
 - When Rebooting, Check Both Drives A: and B: Also checks a floppy disk in drive B: for boot viruses when you shut down your computer. Select this option if you have a system that can boot from a disk in the B: drive.
- 5 Click OK to close the dialog box.
 - 6 Click OK to save your settings and close the dialog box.

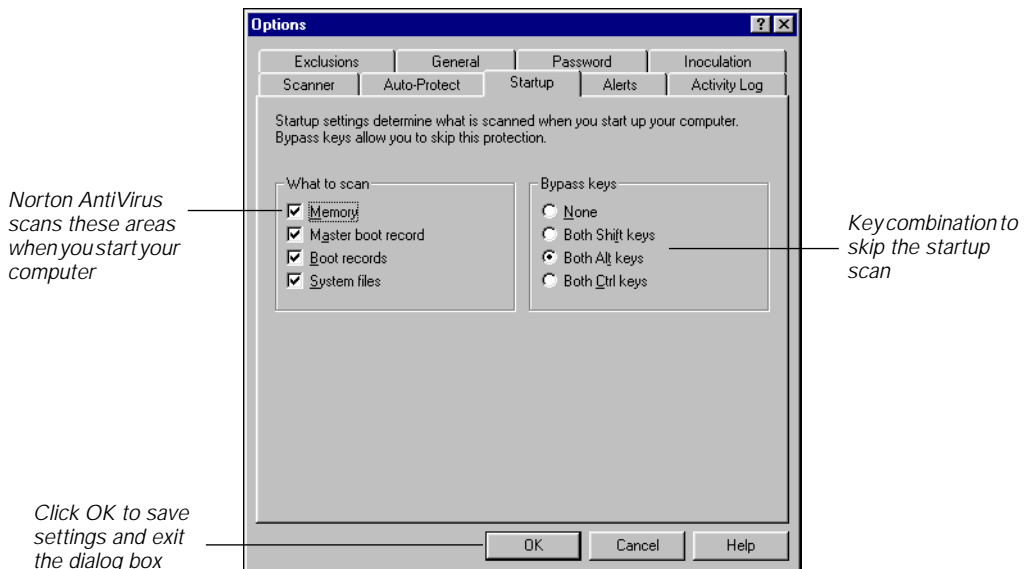
Customizing startup protection

Checking for viruses during system startup is an important step in preventing viruses from activating or spreading. If a system file is infected, the virus will activate when you start up your computer and may infect other programs you run during the day.

To customize system startup protection:

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

Figure 5-13 Startup Settings



- 3 Specify in the What To Scan group box the areas that you want Norton AntiVirus to scan each time you start your computer:
 - Memory: Scans for viruses resident in your computer's memory. Viruses in memory can spread to other files you access.
 - Master Boot Record: Scans for boot viruses in the master boot record.
 - Boot Records: Scans for boot viruses in the boot records on your hard disk.
 - System Files: Scans the operating system files your computer uses to startup and run Windows.
- 4 Specify in the Bypass Keys group box the keystroke combination you want to use to prevent automatic protection from loading when your computer starts up. The bypass key may be useful if you are trying to resolve a system startup problem or configuration conflict.

Select None if you don't want a bypass key combination.
- 5 Click OK.

Customizing inoculation

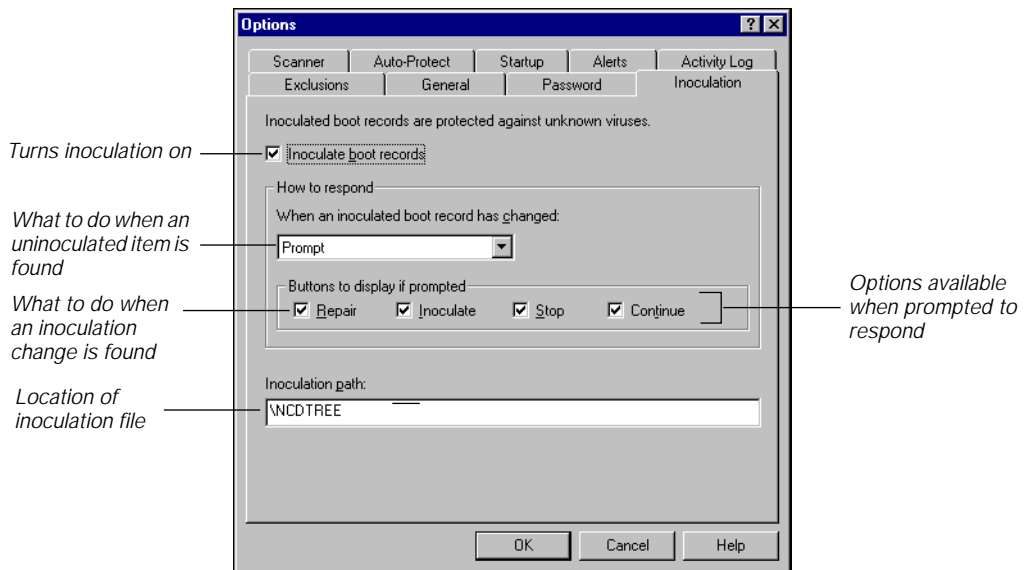
Inoculating boot records offers an extra level of protection against unknown viruses. When you inoculate a boot record, Norton AntiVirus records critical information about it (similar to taking a fingerprint). Subsequently, Norton AntiVirus monitors the inoculated item for changes that could indicate an unknown virus.

Customizing inoculation involves specifying how to respond when a change has occurred.

To enable inoculation protection:

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

Figure 5-14 Inoculation Settings



- 3 Check Inoculate Boot Records so that the master boot record and boot records on your hard disk receive inoculation protection.
- 4 Click OK to save changes and close the dialog box, or continue with the next procedure.

To customize how to respond to inoculation issues:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Inoculation tab (see Figure 5-15).
- 3 Select an option in the When An Inoculated Boot Record Has Changed drop-down list box:
 - Prompt: Informs you when a file or boot record has changed and allows you to choose how to respond.
 - Notify Only - Don't Reinoculate: Merely informs you that the boot record has changed. It does not reinoculate the item.
- 4 If you selected Prompt in step 3, specify in the Buttons To Display If Prompted group box which options you want available when an inoculation issue is found:
 - Repair: Allows you to repair a boot record with an inoculation change, returning the item to its state when it was last inoculated.

- Inoculate: Allows you to inoculate a boot record or reinoculate a changed boot record.
 - Stop: Allows you to stop the current operation (scanning or accessing a file). No change is made to the inoculation data.
 - Continue: Allows you to continue the current operation (scanning or accessing a file). No change is made to the inoculation data.
- 5 Type a folder path for the inoculation files in the Inoculation Path text box.
The default path is \NCDTREE for the inoculation files.
 - 6 Click OK to save your settings and close the dialog box.

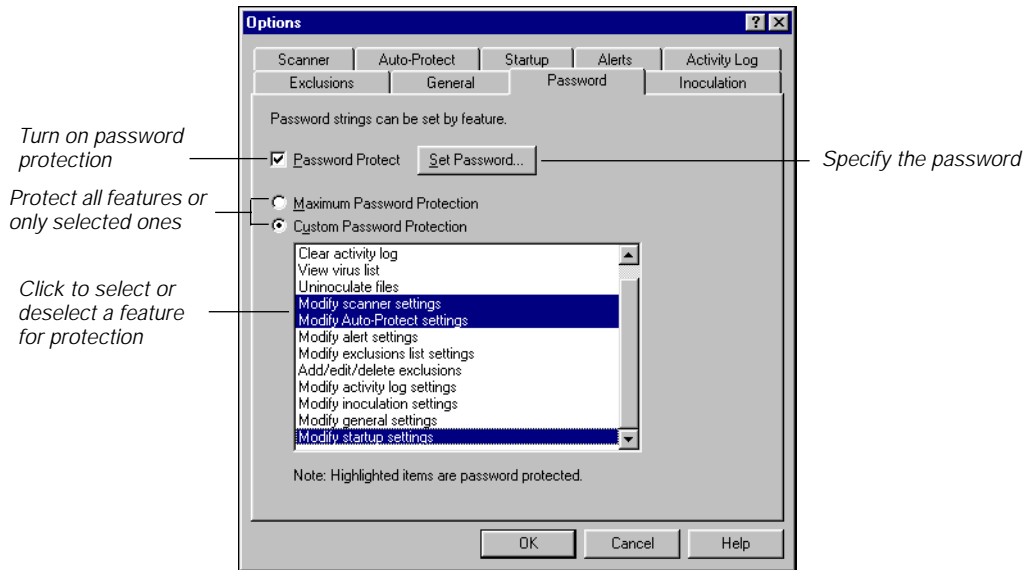
Setting password protection

Password protection guarantees that your Norton AntiVirus configuration will not be modified. You can protect selected features or all configurable options.

To password-protect features:

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

Figure 5-15 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 enter 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.
 - 7 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 5-15).
- 3 Enter your existing password in the Verify Password dialog box that appears.
- 4 Click Set Password.
- 5 Enter your existing password in the Old Password text box.
- 6 Enter the new password in the New Password text box, then type it again in the Confirm New Password text box.
- 7 Click OK.

To remove password protection:

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Password tab (see Figure 5-15).
- 3 Enter 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. Under normal circumstances, 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. See “[Customizing manual scan options](#)” on page 73 and “[Customizing automatic protection](#)” on page 89 for information about configuration options.
- 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 also 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.

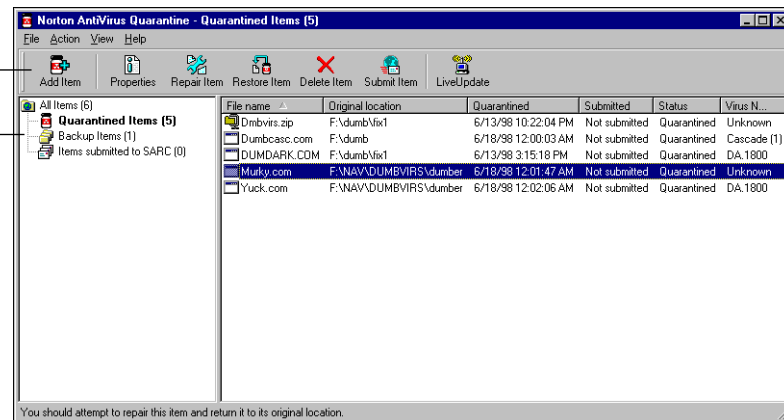
To access the Quarantine, do one of the following:

- 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*

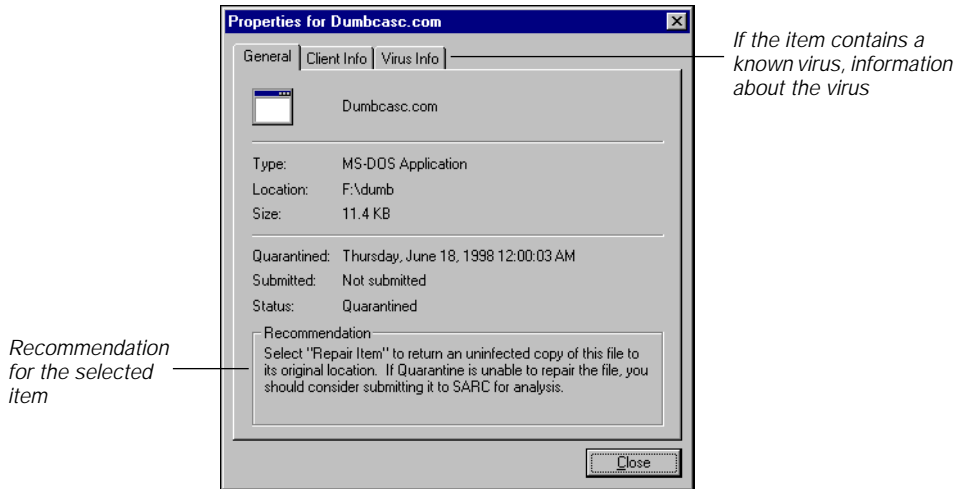
*Types of items
stored in the
Quarantine*



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



To re-scan a file isolated in the Quarantine:

- 1 Open the Quarantine.
- 2 Click LiveUpdate in the Quarantine window.
Your installed set of virus definitions files is updated with the latest definitions automatically.
- 3 Select the file in the Quarantine and click Repair Item.
The file is scanned again with the new definitions.

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.

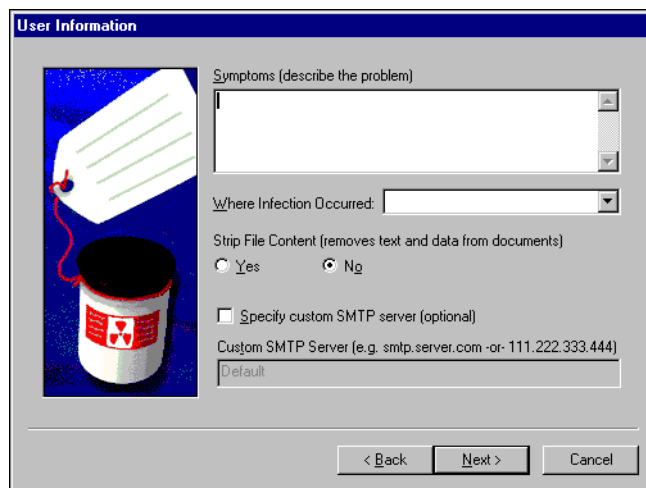
Submitting a file to SARC for analysis

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 'User Information' dialog box. On the left is a graphic of a white tag with a red string tied to a black bucket with a red radiation symbol. The dialog box contains the following fields and options: a text box for 'Symptoms (describe the problem)', a dropdown menu for 'Where Infection Occurred:', radio buttons for 'Strip File Content (removes text and data from documents)' with 'No' selected, a checkbox for 'Specify custom SMTP server (optional)' which is unchecked, and a text box for 'Custom SMTP Server (e.g. smtp.server.com -or 111.222.333.444)' with 'Default' entered. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

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: This option only applies to corporate sites to route submissions through a firewall or who manage virus protection centrally.

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 uncompress (open up) the compressed file. Further, you cannot submit the complete compressed file to SARC for analysis. You must uncompress the file first.

To uncompress for repair or submission:

- 1 Double-click the Norton AntiVirus Auto-Protect icon on the taskbar in the lower-right corner of 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 uncompress the file.
- 4 Add the infected or potentially infected file to the Quarantine.
See “Adding a file to the Quarantine manually” on page 103.
- 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 recompress the file, if desired.
- 7 Double-click the Norton AntiVirus Auto-Protect icon on the taskbar in the lower-right corner of your Windows desktop, then click the Enable button to turn Auto-Protect on 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.

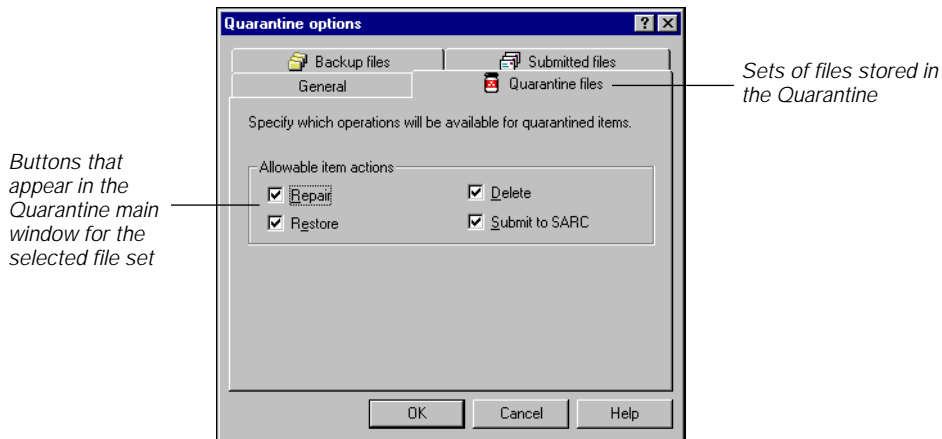
- **Items Submitted To SARC:** Files sent to SARC from the Quarantine for analysis.

You can specify which actions 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

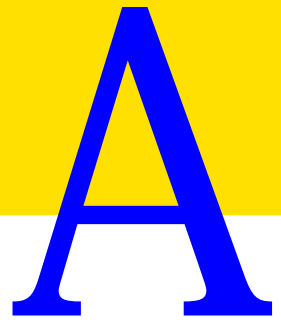


- 3 Click the Quarantine Files, Submitted Files, or Backup Files tabs and check which actions you want to permit for each file set.

If you do not want users to be able to change Quarantine options, you set can 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, over 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. For example,

A virus can infect:

- Program files, non-file areas used on computer startup (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 e-mail message

A virus 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:** 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.
- **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 60 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 newest 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 95/98, 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 95/98	Windows 95/98 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 95/98 may display warnings during startup and your system's performance may degrade.
Windows NT	Windows NT provides the least degree of DOS compatibility, but it still hosts program viruses quite well. 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 95/98, 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 allowed you to 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 merely 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 kicks into action again. 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 in a completely discrete fashion. 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.

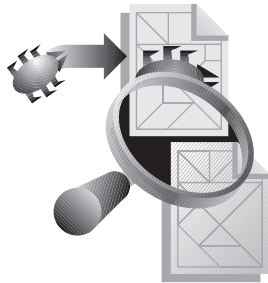
Finally, as far as a macro virus is concerned, the application serves as the operating system. A single macro virus can spread to any of the platforms on which the application is installed and running. For example, a single macro virus that uses Microsoft Word could conceivably spread to Windows 3.x, Windows 95/98, 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

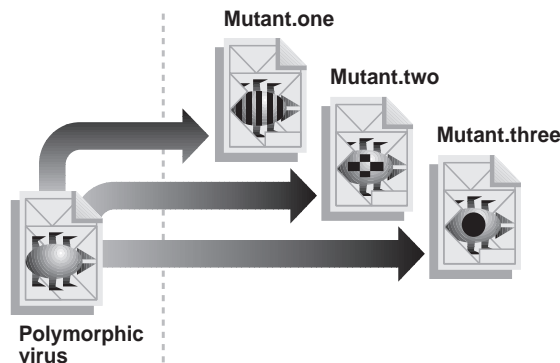
Stealth viruses actively seek to conceal themselves from attempts to detect or remove them. They use techniques such as intercepting disk reads to provide an uninfected copy of the original item in place of the infected copy (read-stealth viruses), altering disk directory or folder data for infected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

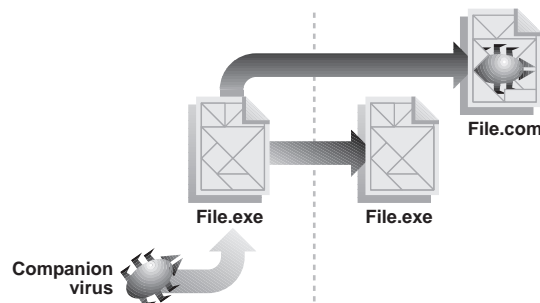
Polymorphic viruses

Most simple viruses attach identical copies of themselves to the files they infect. An anti-virus 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.

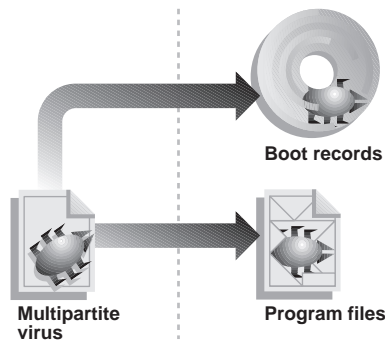


Companion viruses use a variety of strategies. Some companion viruses create a .COM file with a name identical to an existing .EXE file. For example, the companion virus might create a file named CHKDSK.COM and place it in the same directory as CHKDSK.EXE. Whenever DOS must

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. See [Chapter 4, "Keeping up with new viruses,"](#) on page 65 for detailed information and procedures.

The world of computer viruses is a dynamic one. Be sure to update your virus definitions files at least once per month.

Using your Norton AntiVirus Rescue Disks

A Norton AntiVirus rescue disk set simplifies recovery from virus emergencies. The Rescue Disk set is composed of the following three disks:

- Norton Rescue Boot Disk: Used to start your computer.
- Norton AntiVirus Program Disk: Used to scan for and remove viruses.
- Norton AntiVirus Definitions Disk: Virus definitions files used during scans.

If you have not yet created a Norton AntiVirus rescue disk set, do it now. See [“Creating a rescue disk set”](#) on page 39.

Removing viruses from a shutdown computer

To remove viruses using your Norton AntiVirus rescue disk set:

- 1 If your computer is running, choose Shutdown from the Windows Start menu, then switch off your computer using the power switch.
- 2 Place your write-protected Norton Rescue Boot Disk in the A: drive, then switch on your computer.
Slide open the plastic tab on the back of the disk to write-protect it. This prevents a virus from accidentally changing the data stored on the disks.
- 3 After your computer starts, remove the Norton Rescue Boot Disk and insert the Norton AntiVirus Program Disk in the A: drive.

- 4 At the DOS prompt (A:\>), type GO and press Enter.
After a few moments Norton AntiVirus will start.
- 5 Follow the on-screen directions.
You are prompted when it's time to insert the Norton AntiVirus Definitions Disk.

Note: Your mouse won't be working when you use your Rescue Disks. If Norton AntiVirus detects a virus, press the first letter of the action you want to take when prompted. For example, press R for Repair. In most cases, you can simply press Enter to choose the recommended action.

- 6 When the process is complete, remove the rescue disk from the A: drive and restart your computer.

Restoring your hard disk

Caution: The following is an emergency procedure. Before you attempt to restore your hard disk, read the file called VIRSPEC.TXT located in your Norton AntiVirus folder or included with your virus definitions update. This file explains when you should or should not attempt this restoration.

There are a few situations when critical information about your hard disk is damaged by a virus and cannot be repaired. You can use your Norton AntiVirus rescue disk set to recover from these emergencies.

The error message that Norton AntiVirus returns, such as "Unable to repair boot record" or "Unable to repair master boot record," determines how you use your rescue disks. Typically, you restore the CMOS data if your hard disk "disappears" or the number of drives or amount of memory is reported incorrectly:

master boot record partition table	
---	--

	The first physical sector on a hard disk. It contains the master boot record program and the partition table, which stores information about how a hard 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.
--	---

boot records	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.
CMOS	An abbreviation for Complimentary Metal Oxide Semiconductor. A battery-powered chip in 80286 (and more advanced) computers that stores basic data about the system's hardware.

If your rescue disk set is current, it is safe to restore all three items.

Caution: Never use Norton AntiVirus rescue disks that were created for another computer. Rescue disks are specific to the computer for which they were created. Always create new rescue disks for your computer if you install a new operating system and add or change hardware devices, such as hard disks, or increase memory (RAM). See [“Creating a rescue disk set”](#) on page 39 for directions.

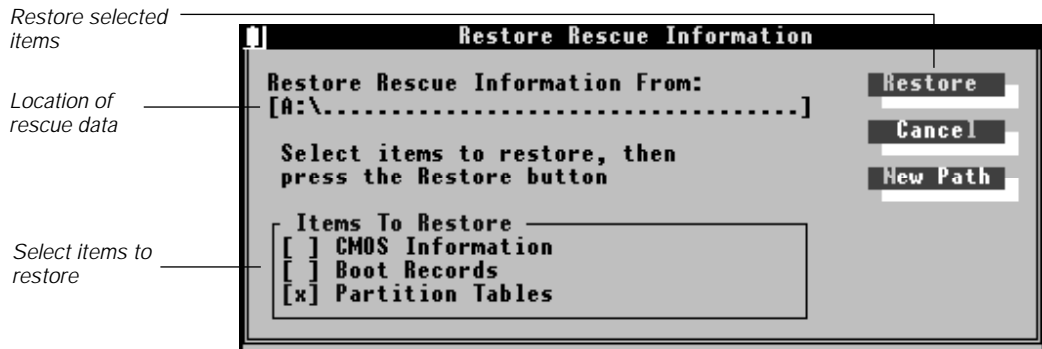
Because the Norton AntiVirus emergency programs run under DOS, not Windows, you have to navigate the dialog boxes using the keyboard. The mouse won't work. Use the following keys to make your selections:

- Press the Tab key to cycle through all of the controls in a dialog box.
- Use the up arrow and down arrow keys to highlight a choice, such as a drive, in a group box.
- Press the Spacebar to check or uncheck a highlighted check box.
- Press Enter to activate the highlighted command button.
- To immediately activate any control or button, press and hold the Alt key, then press the highlighted letter of the control or button label. Release both keys.

To restore your hard disk:

- 1 Switch off your computer using the power switch.
- 2 Place your write-protected Norton Rescue Boot Disk in the A: drive, then switch on your computer.
Your computer will start up from the rescue disk.
- 3 Type RESCUE at the A: prompt and press Enter.
The Restore Rescue Information dialog box appears.

Figure B-1 RESCUE main window



- 4 Make sure A:\ is specified for the location of the rescue data.
- 5 Check the items you want to restore in the Items To Restore group box. Items that are different from the stored information are checked automatically.
Press Tab to move around the dialog box. Press Spacebar to check or uncheck items.
- 6 Select Restore to restore the selected items.
- 7 When the process is complete, remove your Norton Rescue Boot Disk from the A: drive and restart your computer.
- 8 Start Norton AntiVirus and scan all hard drives again. Scan floppy disks as well to try to find the source of the virus.

Using command-line switches

A switch is an abbreviated command that you can use to direct a Norton AntiVirus activity or override default settings. The following Norton AntiVirus components can be run with command-line switches. When run without switches, these components all display a user interface instead:

- NAVDX.EXE performs startup scans and scans for viruses in emergency situations, such as after a virus alert shutdown.
- NAVW32.EXE is the Windows interface and scanner.
- RESCUE.EXE restores hard disk boot records, CMOS settings, and partition tables previously saved on your Norton Rescue Boot Disk. See [“Creating a rescue disk set”](#) on page 39 for directions.

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 pipe symbol (|) means that you should use either parameter, but not both. Do not type the brackets around the parameters on the command line.

NAVDX.EXE



NAVDX.EXE is the Norton AntiVirus component that performs startup scans and is run from the DOS prompt to scan for viruses in emergency situations, such as after a virus alert shutdown. See [“Removing viruses from a shutdown computer”](#) on page 117 for more information.

Syntax

NAVDX [pathname] [options]

pathname	Any drive, folder, file, or combination of these is scanned. If you want to scan a combination of items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files (for example, NAVDX 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 of any folders specified in the pathname.
/M[+ -]	Enables (+) or disables (-) scanning of memory (for example, NAV C: /M+ or NAV D: /M-).
/MEM	Only memory is scanned.
/B[+ -]	Enables (+) or disables (-) scanning of boot records (for example, NAV A: /B+ or NAV B: /B-).
/BOOT	Only the boot records of the specified drives are scanned.
/PROMPT	Informs you when a virus is found and allows you to choose how to respond. The response choices available are determined by the items checked in the Buttons To Display If Prompted group box in the Options - Scanner Settings dialog box. See "Customizing manual scan options" on page 73 for more information.
/REPAIR	Repairs an infected file without notifying you. The result is recorded in the Activity Log.
/DELETE	Deletes an infected file without notifying you. The result is recorded in the Activity Log.
/HALT	Shuts down your computer when a virus is found.
/NOBEEP	NAVDX runs silently.
/ZIPS	Scans files in compressed files
/DOALLFILES	Scans all files, not just executables.

/LOG:file	Creates a new log file.
APPENDLOG:file	Adds to an existing log file.
/CFG[:folder]	Specifies the folder containing program settings.
/HELPERROR	Displays the DOS errorlevel codes that are returned.
/?	Displays a brief description of all command-line switches available for NAVDX.

NAVDX also returns the following DOS errorlevel codes, which can be processed by batch files with the IF ERRORLEVEL statement. See your DOS documentation for more information.

Code	Error
0	No errors occurred and no viruses were found.
10	A virus was found in memory.
11	An internal program error occurred.
13	One or more viruses were found in the master boot record, boot sector, or files.
15	NAVDX self-check failed; it may be infected or damaged.
102	CTRL-C or CTRL-BREAK was pressed to interrupt the Scan.

Examples of usage

To scan all .EXE files in your GAMES folder, type:

```
NAVDX C:\GAMES\*.EXE
```

To scan the GAMES folder on your hard disk, your D: drive, and the file C:\SAMPLES\SAMPLE.EXE, type the following at the DOS prompt:

```
NAVDX C:\GAMES D: C:\SAMPLES\SAMPLE.EXE
```

If C:\SAMPLES is the current folder, type:

```
NAVDX C:\GAMES D: SAMPLE.EXE
```

To scan a folder on the network drive P: called PROGRAMS and all of its subfolders, type:

NAVDX P:\PROGRAMS /S+

If you want to immediately repair any infected files found during this scan, type:

NAVDX P:\PROGRAMS /S+ /REPAIR

To scan memory only, type:

NAVDX /MEM

To scan only the boot records of drives C: and A: type:

NAVDX C: A: /BOOT

NAVW32.EXE



NAVW32.EXE is the Windows interface and scanner. It can be run with command-line switches, typically from the Start menu RUN command, to override configuration settings. When scanning drives using command-line switches, Norton AntiVirus runs minimized, but will pop open on your screen if a virus is found.

Syntax

NAVW32 [[pathname] options]

pathname	Any drive, folder, file, or combination of these is scanned. If you want to scan a combination of items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files (for example, NAVW32 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	All subfolders of any folders specified in the pathname are also scanned.
/M[+ -]	Enables (+) or disables (-) scanning of memory (for example, NAVW32 C: /M+ or NAVW32 D: /M-).
/MEM	Only memory is scanned.

/B[+ -]	Enables (+) or disables (-) scanning of boot records (for example, NAVW32 A: /B+ or NAVW32 B: /B-).
/BOOT	Only the boot records of the specified drives are scanned.
/NORESULTS	No scan results are reported on screen.

Examples of usage

To scan all .EXE files in your GAMES folder, type:

```
NAVW32 C:\GAMES\*.EXE
```

To scan the GAMES folder on your hard disk, your D: drive, and the file C:\SAMPLES\SAMPLE.EXE, use the RUN command and type the following:

```
NAVW32 C:\GAMES D: C:\SAMPLES\SAMPLE.EXE
```

If C:\SAMPLES is the current folder, type:

```
NAVW32 C:\GAMES D: SAMPLE.EXE
```

To scan a folder on the network drive P: called PROGRAMS and all of its subfolders, type:

```
NAVW32 P:\PROGRAMS /S
```

To scan memory only, type:

```
NAVW32 /MEM
```

To scan only the boot records of drives C: and A: type:

```
NAVW32 C: A: /BOOT
```

To specify paths with long filenames that contain spaces, use double quotes:

```
NAVW32 "C:\Homework Helper"
```

RESCUE.EXE



RESCUE.EXE, run from the DOS prompt, restores hard disk boot records, CMOS settings, and partition tables previously saved on your Norton Rescue Boot Disk. See [“Restoring your hard disk”](#) on page 118 for more information.

Tip: If you haven't yet created a Norton AntiVirus Rescue Disk set, do it now. See [“Creating a rescue disk set”](#) on page 39 for directions.

Syntax

```
RESCUE [ /RESTORE[:location]] [ /G0 ] [ /BW | /LCD ]
```

/RESTORE	Restore from a rescue disk.
location	Drive and directory of rescue files.
/G0	Disables graphical mouse and all graphical characters.
/BW	Improves display on black and white monitors.
/LCD	Improves display on LCD monitors.
/?	Displays a brief description of all command-line switches available for RESCUE.

Example of usage

To restore rescue information from the A: drive:

```
RESCUE /RESTORE:A:\
```

System messages

This appendix contains an alphabetical list of the error messages you may see while using Norton AntiVirus. Whenever an item such as <FILENAME>, <DRIVE>, or <VIRUS NAME> appears, it is replaced by an actual filename, drive, or virus name in the message on your screen.

Messages and their meanings

Boot record has changed since inoculation.

Inoculation changes in a boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate. See “[Responding to Inoculation alerts](#)” on page 50 for more information.

The configuration file NAVOPTS.DAT not found.

Norton AntiVirus could not find the file that contains the configuration settings. Norton AntiVirus loaded with the default settings.

Error on drive <DRIVE>. Drive or device not ready.

Norton AntiVirus could not access the specified drive because the drive door is open or there is a problem with the drive.

The <VIRUS NAME> boot virus was found on drive <DRIVE>.

A virus was found in the boot record on the specified drive. To remove the virus, select the Repair command button. For more information, see “[Responding to Auto-Protect virus found alerts](#)” on page 56.

The <VIRUS NAME> virus was found in memory.

A virus was found in your computer's memory, which means it is active and possibly spreading to other files. See [“Responding to Auto-Protect virus in memory alerts”](#) on page 55 for more information.

The boot record of drive <DRIVE> has changed since inoculation.

Inoculation changes in a boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate. See [“Responding to Inoculation alerts”](#) on page 50 for more information.

The boot record of drive <DRIVE> is infected with the <VIRUS NAME> virus.

A virus was found in the boot record on the specified drive. To remove the virus, select the Repair command button. For more information, see [“Responding to Auto-Protect virus found alerts”](#) on page 56.

The boot record on drive <DRIVE> is infected with the <VIRUS NAME> virus. Unable to inoculate boot records and system files.

A virus was found in the boot record on the specified drive. Scan the drive to find and remove the virus, then inoculate the boot records and system files. See [“Scanning for viruses”](#) on page 32 for more information.

The file <FILENAME> in the compressed file <FILENAME> is infected with the <VIRUS NAME> virus.

A virus was found in a file contained within the compressed file. Uncompress the file, then scan the files to find and remove the virus. See [“Responding to Auto-Protect virus found alerts”](#) on page 56 for more information.

The file <FILENAME> is attempting to change the read-only attribute of file <FILENAME>.

Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform. See [“Responding to Auto-Protect virus-like activity alerts”](#) on page 57 for more information.

The file <FILENAME> is attempting to format the hard disk.

Norton AntiVirus is configured to notifying you because this is an activity that viruses sometimes perform. See [“Responding to Auto-Protect virus-like activity alerts”](#) on page 57 for more information.

The file <FILENAME> is attempting to write to <FILENAME>.

Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform. See “[Responding to Auto-Protect virus-like activity alerts](#)” on page 57 for more information.

The file <FILENAME> is attempting to write to the boot record of drive <DRIVE>.

Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform. See “[Responding to Auto-Protect virus-like activity alerts](#)” on page 57 for more information.

The file <FILENAME> is attempting to write to the master boot record of the hard disk.

Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform. See “[Responding to Auto-Protect virus-like activity alerts](#)” on page 57.

The file <FILENAME> is infected with the <VIRUS NAME> virus.

A virus was found in the specified file. To remove the virus you can delete the file or repair the file. See “[Responding to Auto-Protect virus found alerts](#)” on page 56 for more information.

The file <FILENAME> was not allowed to change the read-only attribute of the file <FILENAME>.

Norton AntiVirus is configured to not allow the read-only attribute changes to files because it is an action that viruses sometimes perform. See “[Monitoring for virus-like activities](#)” on page 92 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See “[Scanning for viruses](#)” on page 32 for more information.

The file <FILENAME> was not allowed to format the hard disk.

Norton AntiVirus did not allow the specified file to format your hard disk because it is an action that viruses sometimes perform. See “[Monitoring for virus-like activities](#)” on page 92 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See “[Scanning for viruses](#)” on page 32 for more information.

The file <FILENAME> was not allowed to write to the boot record of drive <DRIVE>.

Norton AntiVirus did not allow the specified file to write to the boot record of the specified disk because it is an action that viruses sometimes perform. See [“Monitoring for virus-like activities”](#) on page 92 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See [“Scanning for viruses”](#) on page 32 for more information.

The file <FILENAME> was not allowed to write to the file <FILENAME>.

Norton AntiVirus is configured to not allow changes to program files because it is an action that viruses sometimes perform. See [“Monitoring for virus-like activities”](#) on page 92 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See [“Eliminating viruses detected during scans”](#) on page 47 for more information.

The file <FILENAME> was not allowed to write to the master boot record of drive <DRIVE>.

Norton AntiVirus is configured to not allow changes to the master boot record because it is an action that viruses sometimes perform. See [“Monitoring for virus-like activities”](#) on page 92 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See [“Eliminating viruses detected during scans”](#) on page 47 for more information.

The master boot record of drive <DRIVE> has changed since inoculation.

Inoculation changes in the master boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate. See [“Responding to Inoculation alerts”](#) on page 50 for more information.

The master boot record of drive <DRIVE> is infected with the <VIRUS NAME> virus.

A virus was found in the master boot record on the specified drive. To remove the virus, select the Repair command button. For more information, see [“Responding to Auto-Protect virus found alerts”](#) on page 56.

The master boot record on drive <DRIVE> is infected with the <VIRUS NAME> virus. Unable to inoculate boot records and system files.

A virus was found in the master boot record on the specified drive. Scan the drive to find and remove the virus, then inoculate the boot records and system files. See “[Eliminating viruses detected during scans](#)” on page 47 for more information.

Not enough memory for desired operation.

Your computer does not have enough conventional memory to load Norton AntiVirus because there are terminate-and-stay-resident programs taking up space in conventional memory.

Unable to access drive: <DRIVE>.

Norton AntiVirus could not access the specified drive because the drive door is open or there is a problem with the drive.

Unable to complete scan.

Norton AntiVirus found more problems (infected files or inoculation changes) than it can report at one time. Correct the problems reported, then scan again. Norton AntiVirus will report any additional problems it finds. See “[Eliminating viruses detected during scans](#)” on page 47 for information on resolving the problems found.

Unable to delete write-protected file <FILENAME>.

The file Norton AntiVirus is trying to delete is on a write-protected disk or in a folder for which you don't have write access.

Unable to find the virus definitions files.

The files that Norton AntiVirus uses to detect known viruses cannot be found. You should reinstall Norton AntiVirus or get updated copies of the virus definitions files. See the “[Automatically updating virus definitions](#)” on page 65 for information on getting updated virus definitions files.

Unable to inoculate boot records on drive <DRIVE>.

Norton AntiVirus cannot inoculate the boot records and system files because of a disk error. Your disk may have cross-linked files or a hardware problem.

Unable to open system messages file.

The system messages files are not in the Norton AntiVirus folder. Reinstall Norton AntiVirus.

Unable to print the requested information.

The data cannot be printed because the printer is not connected or not online.

Unable to read the boot record.

Norton AntiVirus was not able to access the boot record to check it for inoculation. This message can occur if you are using a program that locks the boot record in some way, preventing Norton AntiVirus from accessing it.

Unable to read the master boot record.

Norton AntiVirus was not able to access the master boot record to check it for inoculation. This message probably indicates a hardware problem. This message also occurs if you are using a program that locks the boot record in some way, preventing Norton AntiVirus from accessing it.

Unable to reinoculate boot records on drive <DRIVE>.

The boot records and system files cannot be reinoculated because you don't have read-write access to the inoculation file. See ["Customizing inoculation"](#) on page 96 for information on the location of the inoculation file.

Unable to repair <FILENAME>. The file is still infected with the <VIRUS NAME> virus.

Norton AntiVirus was not able to remove the virus from the specified file. You can eliminate the virus by deleting the file. See ["Responding to Auto-Protect virus found alerts"](#) on page 56 for more information.

Unable to repair boot record of drive <DRIVE>.

Norton AntiVirus was not able to repair a boot record on the specified drive. See ["Restoring your hard disk"](#) on page 118 for more information.

Unable to repair master boot record of drive <DRIVE>.

Norton AntiVirus was not able to repair the master boot record on the specified drive. See ["Restoring your hard disk"](#) on page 118 for more information.

Unable to repair system files.

The system files on your startup drive could not be repaired. To remove the virus, use the DOS SYS command from a write-protected bootable disk to restore the system files to an uninfected state. The SYS command is placed on your Norton Rescue Boot Disk.

Unable to repair the boot record of drive <DRIVE> with inoculation data.

Norton AntiVirus was not able to restore the boot record to its previous state. See [“Restoring your hard disk”](#) on page 118 for more information.

Unable to repair the file <FILENAME>.

Norton AntiVirus was not able to repair the file. It is still infected with an unknown virus. You can eliminate the unknown virus by deleting the file. See [“Responding to Auto-Protect virus found alerts”](#) on page 56 for more information.

Unable to repair the master boot record with inoculation data.

Norton AntiVirus was not able to restore the master boot record to its previous state. See [“Restoring your hard disk”](#) on page 118 for more information.

Unable to repair write-protected boot record of drive <DRIVE>.

The boot record you are trying to repair is on a write-protected floppy disk. Remove write-protection, then repair the boot record.

Unable to update activity log file.

The Activity Log could not be updated because you don't have read-write access to it.

Unable to update exclude file.

The Exclusions List file could not be updated because you don't have read-write access to it.

Unable to update inoculation file.

The inoculation file could not be updated because you don't have read-write access to it.

Unable to update the inoculation file in write-protected folder.

You don't have write access to the folder where the inoculation file resides.

Troubleshooting

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

Solutions to common problems

My Norton Rescue Boot Disk doesn't work

Due to the number of product specific technologies used by manufacturers to configure and initialize hard disks, Norton AntiVirus cannot always create a bootable Norton Rescue Boot Disk automatically. If your Norton Rescue Boot Disk does not work properly, do one of the following:

- If you have a special boot disk for your computer, add it to your Norton AntiVirus rescue disk set. In a virus emergency, boot from that disk (first slide open the plastic tab on the back of the disk to make sure it is write-protected). Remove the disk and insert your rescue disk labelled "Norton AntiVirus Program Disk." At the DOS prompt, type `A:GO` and press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Norton Rescue Boot Disk bootable. Be sure to test your modified Norton Rescue Boot Disk.

Sometimes, your Norton Rescue Boot Disk does not work properly because you have more than one operating system installed, such as Windows NT and Windows 95/98. To modify the disk, do the following:

- Start up from your hard disk, insert your Norton Rescue Boot Disk in the A: drive, and, from a DOS prompt, type `SYS A:` and press

Enter. This transfers the operating system to the rescue disk. Be sure to retest your Norton Rescue Boot Disk.

I've scanned and removed a virus, but it keeps infecting my files.

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

Solution: Scan all floppy disks. See ["Scanning for viruses"](#) on page 32 for directions.

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.

See ["Selecting which files to scan"](#) on page 78 and ["Specifying program file extensions"](#) on page 79 for information on how to change the selection of files for scanning.

Norton AntiVirus automatic protection fails to load when I start my computer.

Cause: Norton AntiVirus configuration settings are not correct.

Solution: See ["Turning Norton AntiVirus Auto-Protect off temporarily"](#) on page 35 for directions to enable Auto-Protect. See also ["Customizing startup protection"](#) on page 95 to make sure memory and boot records are scanned at system startup.

Norton AntiVirus is not notifying me when I attempt to do things that I thought it would not allow, such as writing to a program file.

Cause: The virus-like activity settings are configured to allow this activity.

Solution: Norton AntiVirus does not check for the activity when the option is set to Allow. If you wish to be alerted of the activity, change the setting to Prompt.

See ["Monitoring for virus-like activities"](#) on page 92 for more information.

Cause: The activity is excluded for the file.

Solution: Norton AntiVirus may not be alerting you to the attempt because it has been added to the Exclusions List. That is, you selected the Exclude button in a Norton AntiVirus virus-like activity alert or manually added it to the list. In this case, Norton AntiVirus no longer checks for the excluded file to perform the activity.

See “[Managing exclusions](#)” on page 81 for more information.

Cause: The activity is not one that Norton AntiVirus monitors. The virus-like activities are described in “[Monitoring for virus-like activities](#)” on page 92.

After repairing a program with Norton AntiVirus, it does not work properly.

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

Solution: You should replace the program with an uninfected original.

I can't boot to my A: drive.

There are three likely reasons for this:

Cause: If your computer doesn't check your A: drive first on startup, you need to change settings, usually using your computer's Setup program.

Caution: Be careful when making changes using your computer's Setup program. If you've never used it before, you may want to refer to your computer manufacturer's documentation.

Solution: Complete these steps to change the setting:

Table E-1

1 Reboot your computer.

A message on your screen that looks something like this tells you the key or keys to press to run SETUP:

Press if you want to run SETUP.

2 Press the key or keys to launch the Setup program.

3 Set the Boot Sequence to A: C:.

Setup programs vary from one manufacturer to the next. If you can't find the Boot Sequence option, use the Setup program's help system, refer to the documentation that came with your system, or contact your system's manufacturer.

4 Save the changes, then exit the Setup program.

Cause: You need to use a special Boot Disk for your computer.

Solution: In this case, use the boot disk or startup disk that came with your computer.

Cause: Your computer is set up with more than one operating system, such as Windows NT and Windows 95/98.

Solution: See [“My Norton Rescue Boot Disk doesn’t work”](#) on page 135 for more information.

G L O S S A R Y

application	<i>See</i> program.
AUTOEXEC.BAT	Text file of commands that is executed automatically when your computer starts up. The commands set up the path and prompt, and start certain programs. <i>See also</i> CONFIG.SYS, startup folder.
(to) boot	To start the computer.
bootable disk	Disk that contains the operating system necessary to start, or boot, the computer.
boot record	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	Program that is responsible for loading the operating system.
boot virus	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)	On-line service that allows messaging, electronic mail, and file transfer between computer users via modem.
CMOS	Abbreviation for Complimentary Metal Oxide Semiconductor. A battery-powered chip in 80286 (and more advanced) computers that stores basic data about the system's hardware.
cold boot	Start your computer by switching on the power. A cold boot recycles your computer's random access memory, thus removing any viruses that might be present in memory. <i>See also</i> warm boot.
.COM file	<i>See</i> executable file.
command-line switch	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	Single file or series of files that have been compressed into one file using a compression utility such as PKZIP or LHARC.
CONFIG.SYS	Text file containing commands that configure the system's hardware and that load device drivers. The file is automatically executed by the operating system when you start your computer.
data file	File that is created by or associated with an application and contains no executable code.
device driver	Memory resident program that is loaded from CONFIG.SYS or SYSTEM.INI at startup. <i>See also</i> terminate-and-stay-resident program.
directory	<i>See</i> folder.
download	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	Program that installs a virus on your computer. Droppers are not viruses, they are trojan horse programs. <i>See also</i> trojan horse.
exclusion	Condition or activity that you have instructed Norton AntiVirus to ignore in a particular file. For example, you may want Norton AntiVirus to ignore the DOS FORMAT program when it formats a floppy disk.
.EXE file	<i>See</i> executable file.
executable file	File containing a program that can be launched. Executable files generally have the following extensions: .COM, .EXE, .OVR, .OVL, .DRV, .BIN, or .SYS.
file server	Central disk storage device (or devices) connected to a network that provides network users access to shared applications and data files.
folder	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	File that contains a virus.

inoculate	Generate information or data about a file that can be used to verify the integrity of the file at a later time.
inoculation file	File containing inoculation data that is used during scans to verify file integrity. An inoculation file is created for each drive on which you inoculate files.
known virus	Any virus that Norton AntiVirus can detect and identify by name.
launch	Start or run an application.
.LHA file	Series of files that have been compressed into one file using the LHARC utility.
load	<i>See</i> launch.
macro virus	Virus that infects document files. 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)	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	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	Virus that infects and spreads from both program files and boot records.
operating system	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	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	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	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	Executable file or group of files written for a specific purpose such as word processing or creating a spreadsheet.
program virus	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)	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.
registry	Database maintained by Windows 95/98 to store hardware and software configuration information.
reinoculate	To replace a previously inoculated file’s inoculation data with data for the file in its current state.
repair	To remove a virus from a file and return the file to its original, uninfected state.
scan	Systematic search for viruses that is performed by Norton AntiVirus.
shell	Program that provides the interface between the user and the operating system. In Windows 95/98, the shell maintains the desktop, or graphical user interface.
startup folder	Special folder in your Windows\Start Menu\Programs folder. Programs in this folder run automatically when Windows starts.
stealth virus	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	Folder within a folder.
system disk	<i>See</i> bootable disk.
system files	Files that make up the operating system.
taskbar	Desktop component 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.
terminate-and-stay-resident program (TSR)	Program that loads itself into random access memory (RAM) and remains there so that it can be instantly activated. The TSR is removed from memory when the computer is turned off.
trojan horse	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.
TSR	<i>See</i> terminate-and-stay-resident program.
uninoculate	To remove the inoculation data for a file, folder, or drive. <i>See also</i> inoculate.
unknown virus	Virus for which Norton AntiVirus does not contain a virus definition. <i>See also</i> virus definition.
virus	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.
virus-like activity	Activity or action caused by other software that Norton AntiVirus perceives as the work of a possible unknown virus.
VxD	Virtual device driver. It is an operating system extension that manages a computer resource. Auto-Protect is an example of a VxD.
warm boot	To restart your computer by pressing Ctrl+Alt+Del or shutdown and restart. A warm boot can be detected and

emulated by some viruses, so a virus in memory may still be there when the warm boot is complete. *See also* cold boot.

workstation

Computer that is attached to a network and is not the network server.

write-protected disk

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

Series of files that have been compressed into one file (usually with a .ZIP file extension) using PKZIP.

I N D E X

A

- Activity Log
 - customizing, 86–87
 - filtering entries, 38
 - finding files requiring replacement, 57
 - viewing all entries in, 37
- Activity Log Filter dialog box, 38
- Add Event dialog box, 42
- adding
 - exclusions to exclusions list, 82–84
 - program file extensions, 80
- alert boxes
 - appearance on screen, 27
 - command buttons, 51–58
- alerts
 - adding message to, 85
 - Auto-Protect, 53
 - customizing, 84–85
 - customizing response method, 75–77, 91–92
 - described, 26–28
 - enabling audible alarms, 85
 - responding to
 - Auto-Protect virus in memory, 55
 - Auto-Protect virus-like activity, 57
 - inoculation, 50–51
 - methods of removing viruses, 56–60
 - virus found, 56
 - virus in memory, 59–60
 - sending over Novell NetWare networks, 85
 - situations triggering, 53, 59
 - startup scans, 25, 59
- Alerts tab, 84, 85, 86
- audible alarms, enabling, 42, 69, 85
- Auto-Protect feature
 - described, 25
 - disabling temporarily, 35, 62
 - eliminating viruses detected by, 53–54
 - enabling, 16, 35, 62, 105

- Auto-Protect feature (*continued*)
 - floppy disks, 94–95
 - loading automatically, 35
 - program files, 89–92
 - responding to, 56
 - responding to virus alerts, 53–58
- Auto-Protect icon, 35
- Auto-Protect settings dialog box, 89
- Auto-Protect tab, 89
- avoiding viruses, 29

B

- backup copies
 - infected, 61
 - replacing deleted infected files, 61
- backup files
 - creating before repairing, 88
 - deleting virus-infected, 88
- boot records
 - monitoring for attempts to write to, 94
 - reinoculating, 37
 - repairing infected
 - automatically, 76, 91
 - unsuccessfully, 60
 - scanning
 - manually, 74
 - at startup, 96
 - unable to repair, 63
- boot viruses
 - checking floppy disks for, 94
 - described, 71, 111
 - spread mechanism, 111
 - viewing lists of, 71
- booting
 - floppy drive not set for, 137
 - from Norton Rescue Boot Disk, 63
- bypassing startup
 - protection, 96
 - scans, 36

C

- CD, installing from, 12
- closing
 - Activity Log, 38
 - Scheduler, 41, 44
- command buttons
 - alert box, 51–52
 - Auto-Protect alerts, 51
 - Problems Found dialog box, 51
 - startup scan alerts, 51
- command-line switches, 121–126
- common viruses
 - described, 71
 - viewing lists of, 71
- companion viruses, 114
- compressed files
 - file extension, 61
 - repairing, 62
 - scanning manually, 74
- computer virus
 - definition, 20
 - protection against, 19
 - scanning procedure, 32–34
- copying scheduled scan, 45
- creating Rescue Disk set, 39
- customizing
 - Activity Log, 86–87
 - alerts, 84–85
 - Auto-Protect feature
 - enabling and disabling, 35–36
 - program files, 89–92
 - general scan options, 88
 - inoculation, 96–98
 - manual scan options, 73–77
 - response to alerts, 75–77
 - scan options, 73–78
 - system startup protection, 95–96

D

- deleting
 - exclusions, 84
 - files
 - automatically, 76, 91
 - in response to alerts, 56, 57
 - inability to recover after, 56
 - infected, 61
 - program file extensions, 80
 - scheduled scans, 45
 - virus-infected backup files, 88
- detecting viruses
 - Auto-Protect, 47
 - during scans, 47
- detection methods, virus, 22
- disabling virus protection, 35, 62
- downloads, virus protection during, 13
- drives
 - preselecting for scans, 78
 - scanning, 32
 - at startup, 78
 - network, 78

E

- editing
 - custom alert message, 84
 - exclusions list, 84
 - scheduled scans, 45
- enabling
 - audible alarms, 42, 69
 - Auto-Protect feature, 16
 - automatic loading of, 35
 - scheduled virus scans, 42, 69
 - startup scans, 16
 - virus protection, 62, 105
- excluding files from
 - inoculation alerts, 51
 - known virus detection, 77, 92
 - virus-like activities alerts, 58
- exclusions
 - described, 81
 - removing and modifying, 81–84

exclusions list

- adding entries to, 82–84

- viewing, 81

Exclusions tab, 81

exiting Norton AntiVirus, 31

F

files

- adding to exclusions list, 82–84

- deleting infected, 56, 57, 76, 91

- extensions, 61

- infected, 61

- removing viruses from, 56–57, 60

- requiring replacement, finding, 57

- scanning individual, 15, 33

- selecting for scanning, 78–79

- types infected by viruses, 78

filtering Activity Log entries, 38

floppy disks

- installing from, 12

- monitoring for viruses, 94

- scanning for viruses, 32

- unable to repair boot record, 63

floppy drives, unable to boot from, 137

folders

- excluding from scans, 83

- installation default, 12

formats, hard disk

- as virus-like activity, 93

- excluding from checks for attempted, 83

G

general scanning options, 88

General Settings tab, 88

H

hard disks, attempts to format

- excluding items from checks for, 83

- monitoring for, 93

help, online, 31

I

infected files and boot records

- deleting, 56, 76, 91

- removing viruses from, 56–57, 60

- types of file extensions, 61

infections. *See* virus attacks

inoculation

- alerts, 50–51

- changes

 - expected vs. unexpected, 50

 - viewing reports of, 38

- customizing, 96–98

- described, 25

- file location, 98

- individual files and folders, 37

Inoculation tab, 96

installing

- Norton AntiVirus, 11–17

 - configuration options, 12

 - procedure, 12

- software programs, disabling

 - Auto-Protect, 35

- system requirements, 11

Internet, protection from viruses on, 13

K

known viruses, 23

- See also* unknown viruses; viruses

- viewing list of, 70

- viewing report of detections, 37

L

LiveUpdate

- description, 66

- installing, 13

- obtaining, 60

loading

- Auto-Protect feature automatically, 35

- Scheduler at Windows startup, 43

M

- macro viruses, 112
- malicious programs, 71
- manual scans
 - about, 25
 - customizing, 73–77
 - described, 24
- master boot record
 - restoring, 62
 - scanning
 - at startup, 96
 - manually, 74
- memory
 - removing viruses from, 55, 59
 - responding to alerts of viruses in, 55, 59–60
 - scanning
 - manually, 74
 - at startup, 96
- messages, system, 127–134
- monitoring for virus-like activities, 92–94
- multi-boot system, modifying Rescue Disks for, 135
- multipartite viruses
 - described, 71, 115
 - viewing lists of, 71

N

- Netscape plug-ins, 13
- network alerts
 - sending to Norton AntiVirus for NetWare NLM, 85
 - setting alert options, 86
- network drives
 - enabling scanning of, 78
 - restrictions on scanning, 78
- New Exclusion dialog box, 83

- Norton AntiVirus
 - exiting, 31
 - installing, 11–17
 - configuration options, 12
 - options, 12
 - procedure, 12
 - recovering from virus emergencies, 117–120
 - starting, 15, 30
 - uninstalling, 14
 - virus protection technologies, 23–26
- Norton AntiVirus main window, 15
- Norton Rescue Boot Disk, troubleshooting, 135

O

- online help, 31

P

- password protection
 - changing password, 100
 - custom, 99
 - maximum, 99
 - removing, 100
 - setting, 98–100
- Password Settings tab, 99
- payload, virus, 109
- plug-ins, Netscape, 13
- polymorphic viruses
 - described, 71, 114
 - viewing lists of, 71
- preventing virus attacks, 22
 - See also* virus attacks
- printing
 - Activity Log, 38
 - virus lists, 71
- Problems Found dialog box, 50

- program file extensions
 - resetting list of, 81
 - specifying for scans, 75, 79–81
 - viewing current, 79–80
- Program File Extensions dialog box, 80
- program files
 - deleting after virus detection, 92
 - enabling scans of, 75
 - removing viruses from, 90–92
 - scanning only, 79, 90
- program viruses
 - described, 71, 110
 - spread mechanisms, 110
 - viewing lists of, 71
- programs, malicious, 71
- protection
 - avoiding viruses, 29
 - floppy disk exchange, 94

R

- record, 63
- recovering from virus emergencies, 22
- reinoculating files and boot records, 37
- removing
 - program file extensions, 80
 - viruses
 - boot records, 56–57, 60
 - files, 56–57, 60
 - from files and boot records, 56–58, 60
 - from memory, 55, 59
 - master boot record, 56–57, 60
- removing viruses, 61
- Repair Wizard
 - described, 48
 - eliminating viruses
 - automatically, 47
 - detected during scans, 47–51
 - manually, 47
- repairing
 - boot records, 56–57
 - files, 56–57
 - master boot record, 56–57

- repairing files and boot records
 - after inoculation changes, 97
 - compressed, 62
 - manual scans, 76, 91
 - in response to alerts, 56, 60
- repairing infected boot records, 56
- reports, viewing activity, 37–39
- Rescue Disks
 - creating, 14, 39
 - troubleshooting, 135
- responding to virus in memory alerts, 59
- restoring deleted files, warning for, 56

S

- Scanner Advanced Settings dialog box, 77
- Scanner Settings dialog box, 74
- Scanner tab, 73
- scanning
 - drives, 32
 - files, 33
 - installation options, 12
- scanning for viruses
 - copying scheduled scan, 45
 - customizing
 - general scanning options, 88
 - specifying program file extensions, 79–81
 - network drives, 78
 - scheduling, 40–45
 - stopping scans, 78
 - viewing date/time occurred, 38
- Scheduler
 - accessing, 41
 - closing, 44
 - copying scheduled scan, 45
 - disabling, 41
 - loading when starting, 43
 - managing scheduled events, 45
 - scheduling scans, 41
- Scheduler Options Settings dialog box, 44
- searching for virus names, 71
- Set Password dialog box, 99

- Setup program, changing drive boot sequence, 137
- shutting down computer, virus detection during, 76
- Specifying program file extensions, 79
- starting Norton AntiVirus, 15, 30
- startup scans
 - bypassing, 36, 96
 - customizing, 95–96
 - described, 25
 - eliminating viruses detected during, 59–63
 - enabling, 16
- Startup tab, 95
- stealth viruses
 - described, 71, 113
 - viewing lists of, 71
- subfolders, excluding from scans, 83
- system files
 - changes to, 51
 - irreparable, 63
 - reinoculating, 37
 - scanning on startup, 96
 - unable to repair, 63
- system messages, 127–134
- system requirements, 11

T

- trigger, virus, 109
- troubleshooting problems, 135–137

U

- uncompressing files for repair, 62, 105
- uninstalling Norton AntiVirus, 14
- unknown viruses
 - described, 23
 - inoculating against, 37
- updates, virus definitions, 23, 26, 69

V

- viewing
 - Activity Log, 37–39
 - exclusions list, 81
 - scheduled scans, 41
 - virus list, 70–72
- virus attacks
 - See also* preventing virus attacks
 - mechanisms of, 22
 - preventing, 29
 - sources of, 22
- virus definitions, updating, 23, 26, 65–70
- virus list
 - changes to, 38
 - viewing and printing, 70–72
- Virus List dialog box, 70
- virus protection
 - disabling, 35, 62
 - enabling, 35, 62, 105
- virus signatures, 23, 26
- viruses
 - about, 108
 - avoiding, 29
 - deleting infected files, 52, 56–57
 - detecting, 47
 - eliminating
 - automatically with Repair Wizard, 47–51
 - during scans, 47–51
 - with command buttons, 51
 - in memory, 55, 59–60
 - life cycle, 21–22
 - payloads, 109
 - protection, 19
 - removing from memory, 55, 59
 - repairing infected boot records, 56
 - repairing infected files, 52, 56
 - responses to alerts, 51–58
 - sources of, 22
 - spread mechanisms, 22
 - targets of infection, 110

viruses (*continued*)

- triggers, 109

- viewing names and descriptions of,
70–72

virus-like activities

- monitoring for, 92–94

- responding to Auto-Protect alerts of,
57–58

- viewing Activity Log reports of, 38

