# Norton AntiVirus™ Scanner for Windows® NT User's® Guide

SYMANTEC.™

NORTON ANTIVIRUS™

# Norton AntiVirus™ Scanner for Windows® NT User's Guide



## Copyright Notice



## Trademarks



Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# Credits

## Software Development

David Allee, Darren Chi, Alexander Freylicher, Barry Gerhardt, Carey Nachenberg, Yoko Vang, and Gary Westerland

## Product Management

Lily Duong, Jeff Leeds, Sharon Ruckman, and Germaine Ward

## Quality Assurance

Bob Kolosky, John M. Moldenhauer, Sam Porterfield, Ken Sackinger, Francia Saplala, and Ray Waldin

## Documentation and Online Help

Elizabeth Anders, Kurt Ament, Annette Brown, Alfred Ghadimi, Karen Goldsmith, Robert Hoffman, Romey Keys, Sheelagh O'Connor, Vickie Von Bergen, and Laura Weatherford

## Technical Support

Caroline Cento, Michael Fischer, Christine Frazer, Brett Johnson, Todd Kieser, and Michael Logue

## Engineering Services

Ardeshir Babak, Will Jobe, Jo Anne Johnson, and James Reardon

## Virus Definitions

Jonathan Allee, Gioconda Becerra, Chris Brown, Matt Candelaria, Shane Coursen, Philip DeBats, Don Duperault, Chris Formulak, Kevin Marcus, Charles Renert, David Shannon, Jeffrey Sulton, and John Wilber

## External Test

Alena Cespivova, Jo Anne Johnson, and Robert Stones

## SWAT Team

Eric Gustafson, Ron Hayes, Neils Johnson, Howard Mora, Dan Sackinger, and Scott Smith

THIS PAGE LEFT BLANK INTENTIONALLY

# NOW THAT YOU'VE ACCESSED THE WORLD'S BEST SOFTWARE, WHY NOT ACCESS THE WORLD?

**FREE INTRODUCTORY OFFER ON COMPUSERVE**

CompuServe® is the most powerful online service available, offering a wide variety of services and forums to over 1,000,000 active members worldwide. You can be a part of it with Symantec's Free Introductory Membership offer. All you need is a personal computer, telecommunications software, and a modem, and you can take advantage of all these powerful features:

**ONLINE COMPUTER SUPPORT**

**ELECTRONIC BROKERAGE SERVICES**

**ELECTRONIC MAIL AND FAX**

**ONLINE INTERACTION WITH THOUSANDS OF OTHER USERS**

**ACCESS TO HUNDREDS OF DATABASES**

One more powerful reason
to take advantage of this free offer…

# THE SYMANTEC FORUM

## GET ONLINE WITH SYMANTEC™ AND COMPUSERVE.

Now, there's a powerful, new channel of communication between Symantec and our customers. It's the Symantec Forum on the CompuServe Information Service, and it's a great way to stay on top of the latest information and ideas from Symantec.

The Symantec Forum is our way of making sure you get the most out of your Symantec software. Whether you're a novice user or an expert, we want to answer your questions, hear your suggestions, and know what you're thinking about your Symantec products.

## SYMANTEC REPRESENTATIVES AND USERS ARE AS CLOSE AS YOUR KEYBOARD.

With the Symantec Forum, you can interact with Symantec customer service representatives, who are available to answer your questions about any of our products.

It's never been so easy to get answers to your questions and share information with other users.

What's more, the Symantec Forum gives you valuable, up-to-the-minute information, such as:

- Technical Bulletins
- Trial Offers and Demo Software
- Product Add-Ons
- New Symantec Products
- Upgrade Information
- Sample Code
- Tips and Shortcuts
- Training Workshop Dates

## IT'S FOR SYMANTEC CUSTOMERS ONLY, AND IT'S ABSOLUTELY FREE!

If you are already a CompuServe member, simply enter GO SYMANTEC at any prompt to enter the Symantec Forum. This free offer is limited to first-time subscribers only. One per customer. Original reply cards only, please; copies will not be accepted.

# YES!

# I WANT TO GET ONLINE WITH SYMANTEC.

Become a member of CompuServe today, and be a part of the Symantec Forum.
Complete, cut out, place in an envelope, and mail the coupon to the address below and you'll receive:

- **A PRIVATE USER ID NUMBER AND PASSWORD**
- **$15.00 INTRODUCTORY USAGE CREDIT**
- **A COMPLEMENTARY SUBSCRIPTION TO *COMPUSERVE MAGAZINE,* COMPUSERVE'S MONTHLY COMPUTING MAGAZINE**

## TO GET ONLINE EVEN FASTER, CALL TOLL-FREE 1-800-848-8199 AND ASK FOR REPRESENTATIVE #124. OUTSIDE THE U.S. AND CANADA, CALL 1-614-457-0802.

**United States and Canada**
CompuServe Information Services
Department 124
P.O. Box 20212
Columbus, OH 48220-9988
Telephone: 1-800-848-8199, ask for representative #124
**Mexico**
(+52) (5) 629-8190

## FREE INTRODUCTORY COMPUSERVE RESPONSE CARD — MAIL IN TODAY!

Name_____

Address_____

City _____ State _____

Country _____ Zip/Postal Code _____

Phone _____

SYMANTEC.™

THIS PAGE LEFT BLANK INTENTIONALLY

# SYMANTEC LICENSE AND WARRANTY

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

• You may:

(i) use one copy of the Software on a single computer;

(ii) make copies of this Software available to other end users provided that (a) you do not receive any remuneration for such transfer and (b) such end users agree to the terms and conditions of this license and warranty.

• 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; or

(iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

• 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.

THIS PAGE LEFT BLANK INTENTIONALLY

# Contents

## Quick start


Installing Norton AntiVirus ..... 15
Scanning for viruses ..... 16
Making sure you are protected ..... 17


## About Norton AntiVirus


What is a computer virus? ..... 19
Potential virus damage ..... 19
How Norton AntiVirus protects you ..... 21
How Norton AntiVirus warns you ..... 21
Virus risk under Windows NT ..... 22
    Boot viruses ..... 22
    Program viruses ..... 22
Security considerations ..... 23
MS-DOS and Windows NT ..... 24


## Installing Norton AntiVirus


Installing Norton AntiVirus ..... 27
What to do after installation ..... 28
Uninstalling Norton AntiVirus ..... 29
Getting help ..... 29


## Using Norton AntiVirus


Tips to avoid viruses ..... 33
Starting and exiting Norton AntiVirus ..... 33
Scanning for viruses ..... 34
    Working with scan results ..... 35
        Problems found dialog box ..... 36
        Virus alert dialog box ..... 36
        Scan Results dialog box ..... 37
    Selecting which files to scan ..... 38
        All files ..... 38
        Program files ..... 38
    Bypassing boot record scans ..... 39
Scheduling virus scans ..... 40
Viewing the Activity Log ..... 41
    Filtering Activity Log entries ..... 42
Using command-line switches ..... 43

## Eliminating viruses

Problems found ....45
What to do next ....45
Responding to problems found or virus alerts ....47
What to do if repair is unsuccessful ....49
Dealing with common problems ....50

## Keeping up with new viruses

Updating virus definitions ....53
Virus definitions update sources ....53
CompuServe ....53
America Online ....53
Internet ....54
Microsoft Network ....54
Symantec BBS ....54
Virus definitions update disks ....55
Installing new virus definitions files ....55
Viewing the Virus List ....56

## Customizing Norton AntiVirus

Customizing the scanner ....59
Setting advanced options ....62
Specifying program file extensions ....63
Setting backup options ....64
Managing exclusions ....65
Customizing the Activity Log ....67
Customizing alerts ....69

## System messages

Messages and their meanings ....71

## Emergency recovery

Virus hotline ....75
When you can't start your computer ....75

## Glossary

## Symantec Service and Support Solutions

# Quick start

This section is for experienced computer users who are already familiar with other versions of Norton AntiVirus (NAV). It summarizes the steps to install the Norton AntiVirus Scanner for Windows NT and initiate virus scans.

## Installing Norton AntiVirus

The Norton AntiVirus Scanner for Windows NT is distributed in three different ways: floppy disks, CD-ROM, or a self-extracting compressed file that you download from an online service or bulletin board.

The installation procedure for each is essentially the same. Simply read each installation screen, follow the instructions, then click Next to continue. Click Finish at the end to complete the installation.

### To install Norton AntiVirus from floppy disks:

1. Insert Norton AntiVirus Disk 1 into your floppy disk drive.
2. Choose RUN from the File menu.
3. Type `A:SETUP` in the text box and click OK.

### To install Norton AntiVirus from a CD-ROM disk:

1. Insert the Norton AntiVirus CD-ROM disk into your CD-ROM drive.
2. Choose RUN from the File menu.
3. Type `D:SETUP` in the text box and click OK.

   If your CD-ROM drive uses a different letter, substitute as appropriate.

### To install Norton AntiVirus from a downloaded file:

1. Download "NAVNTSCN.EXE," the self-extracting compressed file, into a temporary directory; for example, C:\TEMP
2. Choose RUN from the File menu.
3. Type `C:\TEMP\NAVNTSCN` in the Run dialog text box and click OK.

   The Norton AntiVirus installation files are extracted automatically.
4. Choose RUN from the File menu.
5. Type `C:\TEMP\SETUP` in the Run dialog text box and click OK.

# Scanning for viruses

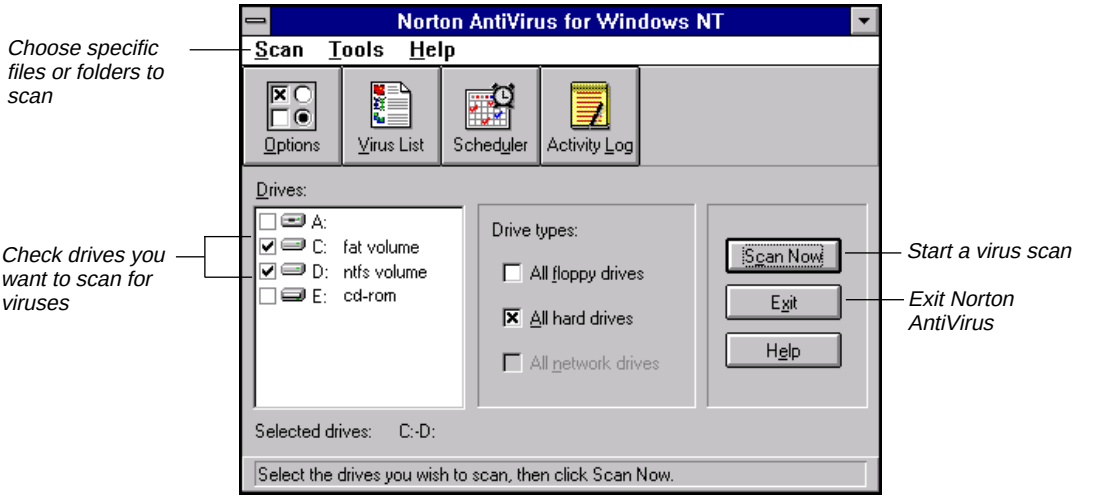
You can scan drives, folders, or specific files for viruses. If Norton AntiVirus finds a virus, see Chapter 4, "Eliminating viruses," for instructions on how to proceed.

### To start Norton AntiVirus:

- Double click Norton AntiVirus Scanner in the Norton AntiVirus program group.

  The Norton AntiVirus window appears.

**Figure 1** Norton AntiVirus main window




### To scan one or more drives:

- Check the specific drives to scan in the Drives list box and click Scan Now. You can check more than one drive.

### To scan a specific file:

- Choose FILE from the Scan menu in the Norton AntiVirus main window.

### To scan a specific folder:

- Choose FOLDERS from the Scan menu in the Norton AntiVirus main window.

# Making sure you are protected

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

- Scan all hard disk drives at least once per week to verify they are virus-free. Schedule the scans to occur automatically so that you don't forget.
- Scan all new files and floppy disks before first use.
- Update your virus definitions regularly to make sure you are protected against newly discovered viruses. A new definitions file is available monthly. See "Updating virus definitions" in Chapter 5 for information on how to receive the files.
- Make periodic backups of your hard disk.
- Use legal copies of all software and make write-protected backups.

---

**NOTE:** If you performed a complete installation and accepted the recommended options, an automatic scan of your startup hard disk is scheduled to run Fridays at 8:00 in the evening.

---

THIS PAGE LEFT BLANK INTENTIONALLY

# About Norton AntiVirus

Norton AntiVirus Scanner for Windows NT is the most effective virus detection and elimination software available for your computer. Use Norton AntiVirus to scan an entire disk (or disks), a particular folder and all of its files, or a specific file for virus infection.

## What is a computer virus?

A computer virus is, simply, a computer program written by an ill-intentioned programmer. Computer viruses infect executable files, such as word processing programs, spreadsheet programs, computer games, or operating system programs. Viruses can also "infect disks" by attaching themselves to special programs in areas of your disks called *boot records* and *master boot records*. These are the areas where the programs your computer uses to start up reside.

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 disk. A computer virus, like a biological virus, lives to replicate.

## Potential virus damage

Some computer viruses, in addition to replicating, 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.

Computer viruses do not infect or damage hardware, such as keyboards or monitors. Though you may suffer 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. Not even your disks themselves are physically damaged, just what's stored on them. Viruses can only infect files and corrupt data.

**Table 1-1** Virus life cycle

| | | |
|---|---|---|
| Infection | **Source** | • Reused floppy disks from unknown sources<br>• Disks from home or school<br>• Disks borrowed from friends<br>• Programs from BBSs or online services<br>• Bargains (from non-reputable dealers)<br>• Re-shrink-wrapped or opened software<br>• Pirated software<br>• Preformatted floppy disks |
| | **Infection** | • Boot from infected disk<br>• Reboot with infected floppy disk left in drive<br>• Run infected program |
| | **Spread** | • Share disk or infected program<br>• Log on to network |
| Detection | **Observation** | • Operating system won't load<br>• Strange system behavior<br>• Files missing or programs not working |
| | **Utility** | • Virus detected by antivirus software |
| Recovery | **Cleanup** | • Reinstall programs from master disks<br>• Repair files with antivirus software<br>• Restore from uninfected backup |
| | **Followup** | • Rescan all files to find source of infection<br>• Scan all floppies to find source of infection<br>• Discard backups that may be infected<br>• Scan more frequently for a while |
| Prevention | Scan floppy disks and new files before first use and scan hard disks at least once per week. | |

# How Norton AntiVirus protects you

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—initiated with the Scan Now button in the main window or scheduled to run automatically—it searches your files for these telltale signatures. If a file is found that has been infected by one of these viruses, Norton AntiVirus has the tools to eliminate the virus automatically.

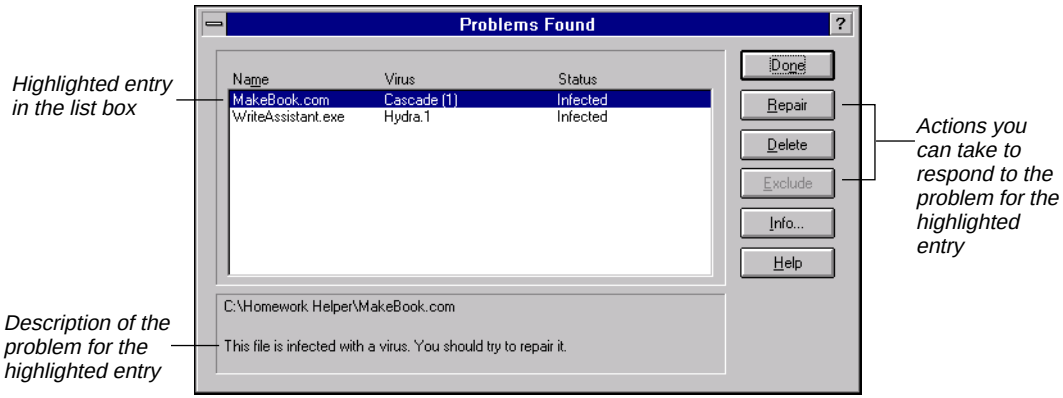
Each time a new virus is discovered, its virus signature is added to the virus definitions file by the Symantec engineers. For this reason, you should update your virus definitions file regularly (a new file is available monthly from Symantec) so that Norton AntiVirus has the needed information to find all known viruses. See "Updating virus definitions" in Chapter 5 for information on how to get regular updates of the virus definitions files.

Don't wait for a virus attack before scanning. Scan regularly to verify that your computer is virus-free. For information on how to scan files, folders, or drives, see "Scanning for viruses" in Chapter 3.

# How Norton AntiVirus warns you

Norton AntiVirus notifies you of viruses by displaying a Problems Found dialog box at the end of a scan. Figure 1-1 shows an example.

**Figure 1-1** Problems Found dialog box




See Chapter 4, "Eliminating viruses," for detailed information on how to respond when a virus is detected.

# Virus risk under Windows NT

There are two main types of viruses:

- Program viruses, which infect application, operating system, and other executable files.
- Boot viruses, which infect the boot record on floppy disks and both the boot record and master boot record on hard disks.

Some viruses, called multipartite viruses, fall into both categories. They can infect program files, boot records, and master boot records.

## Boot viruses

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

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

Windows NT manages memory differently than MS-DOS. If Windows NT can load—despite a boot virus infection, the virus is disabled in memory. Your computer is still infected, but the virus does not show its usual symptoms or spread while Windows NT is running. Many times, however, you won't be able to start up at all. If you boot into MS-DOS on a multi-boot system, the virus is not disabled. All disks, including floppies, are at risk.

## Program viruses

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

Under Windows NT, DOS programs are run in DOS memory space. While in memory, they continue to infect other programs and can interfere with normal operations. Generally, program viruses remain active in your

computer's memory after an infected program is executed until you end the DOS session.

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

---

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

---

## Security considerations

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

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

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

In order to scan boot records, administrator-level rights are required in any configuration. For standalone computers, this is generally the case. For other configurations, it becomes the administrator's responsibility.

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

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

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

**Table 1-2** Boot record access privileges

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

**Table 1-3** Folder access privileges

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

**Table 1-4** File access privileges

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

## MS-DOS and Windows NT

Many computers are configured to permit booting into either Windows NT or MS-DOS. As you might expect, virus exposure is greatly increased. For example, viruses that cannot infect because Windows NT restricts access to

boot records, have free reign under MS-DOS. Further, a boot virus infection from a DOS session may prevent Windows NT from loading at all.

To supplement the Norton AntiVirus Scanner for Windows NT, Symantec provides a free MS-DOS scanner for use in emergency situations, such as when a virus prevents Windows NT from loading. The Norton AntiVirus Scanner for DOS (NAVSCAN.EXE) is available to download from all of the on-line services described in Chapter 5, “Keeping up with new viruses.” The README.TXT file that accompanies the file provides detailed information about its use.

THIS PAGE LEFT BLANK INTENTIONALLY

# Installing Norton AntiVirus

This chapter explains how to install Norton AntiVirus on your computer's hard disk and outlines what you should do after installation is complete.

## Installing Norton AntiVirus

The Norton AntiVirus Scanner for Windows NT is distributed in three different ways: floppy disks, CD-ROM, or a self-extracting compressed file that you download from an online service or bulletin board.

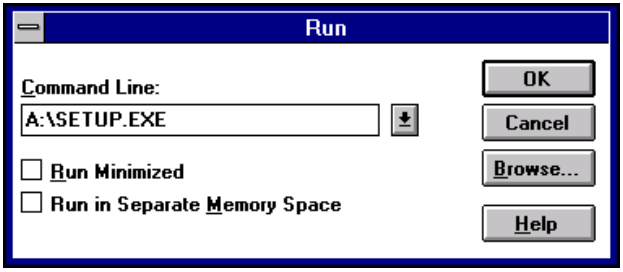
The installation procedure for each is essentially the same. Simply read each installation screen, follow the instructions, then click Next to continue. Click Finish at the end to complete the installation.

### To install Norton AntiVirus from floppy disks:

1. Insert Norton AntiVirus Disk 1 into your floppy disk drive.
2. Choose RUN from the File menu.

   The Run dialog box appears (Figure 2-1).

**Figure 2-1** Run dialog box




3. Type `A:SETUP` in the text box and click OK.
4. Follow the on-screen instructions to complete the installation.

### To install Norton AntiVirus from a CD-ROM disk:

1. Insert the Norton AntiVirus CD-ROM into your CD-ROM drive.
2. Choose RUN from the File menu.
3. Type `D:SETUP` in the text box and click OK.

   If your CD-ROM drive uses a different letter, substitute the appropriate drive letter.
4. Follow the on-screen instructions to complete the installation.

### To install a downloaded version of Norton AntiVirus:

1. Download "NAVNTSCN.EXE," the self-extracting compressed file, into a temporary directory; for example, C:\TEMP
2. Choose RUN from the File menu.
3. Do one of the following:
   - Click Browse to locate NAVNTSCN.EXE in the temporary directory, then click OK in the Run dialog box.
   - Type `C:\TEMP\NAVNTSCN` in the Run dialog text box and click OK.

   The Norton AntiVirus installation files are extracted from the compressed distribution file automatically.
4. Choose RUN from the File menu.
5. Do one of the following:
   - Click Browse to locate SETUP.EXE in the temporary directory, then click OK in the Run dialog box.
   - Type `C:\TEMP\SETUP` in the Run dialog text box and click OK.
6. Follow the on-screen instructions to complete the installation.

## What to do after installation

Here's a list of *important* steps you can take to combat computer viruses:

- Scan all new files and floppy disks before using them for the first time.

  See "Scanning for viruses" in Chapter 3 for instructions.
- Scan your hard disks at least once per week to verify that they are virus-free. Schedule the scans to occur automatically so that you don't forget.

  See "Scheduling virus scans" in Chapter 3 for directions.

- Update virus definitions regularly so that you maintain maximum protection against new viruses. A new file is available monthly.

  See "Updating virus definitions" in Chapter 5 for information on how to get regular updates of the virus definitions files.

# Uninstalling Norton AntiVirus

Norton AntiVirus includes an uninstall tool.

### To uninstall Norton AntiVirus:

- Double click Uninstall Norton AntiVirus in the Norton AntiVirus program group and follow the on-screen instructions.

# Getting help

Online help is provided for all capabilities of Norton AntiVirus. You can get help on concepts, definitions, and procedures by:

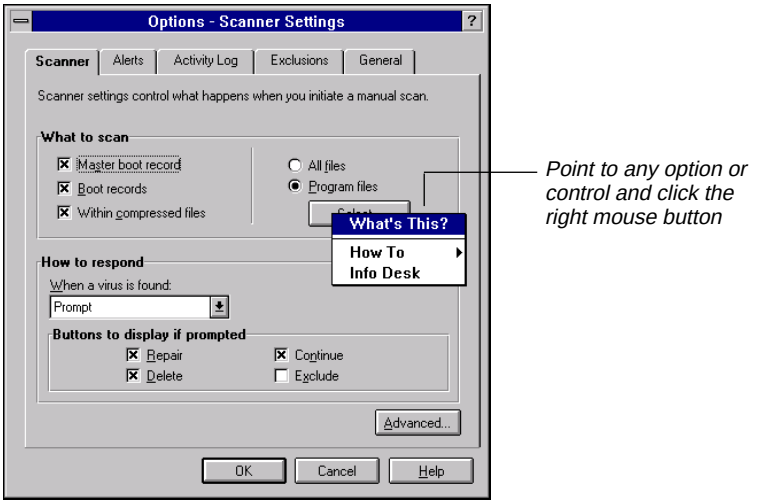
- Clicking the right mouse button on items in a dialog box
- Using commands on the Help menu
- Clicking the help button in a dialog box

The help system includes a table of contents, an extensive topics index, and a glossary. From the help window you can search for, print, annotate, and establish bookmarks for specific help topics. You can also access context-sensitive help for any option in Norton AntiVirus.

### To access context-sensitive help:

1. Position the mouse pointer over an option and click the right mouse button. The help pop-up menu appears (Figure 2-2).

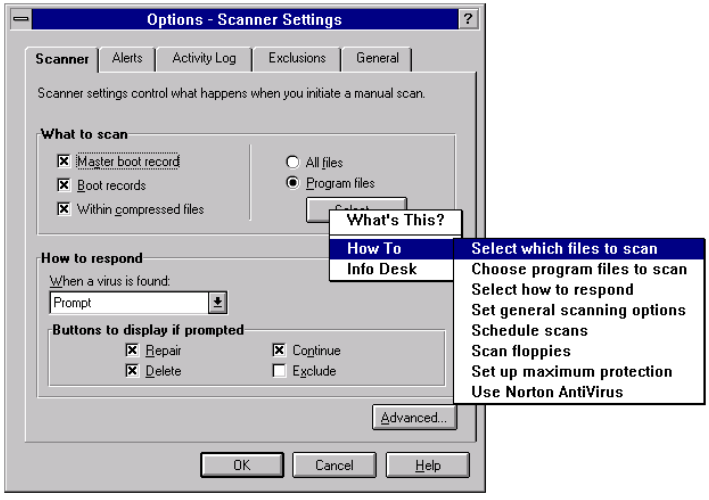
**Figure 2-2** Right mouse button help menu




**2** Do one of the following:

- Choose WHAT'S THIS? to see a brief description of the option.
- Choose HOW TO to display another menu of choices related to that option (Figure 2-3).

**Figure 2-3** How To help menu



Another way to access context-sensitive help for an option in a dialog box is through the question mark (?) icon in the title bar of any dialog box.

### To get help about options:

1. Click the question mark (?) icon in the title bar of any dialog box.

   A question mark appears next to the mouse pointer.

2. Click any option in the dialog box.

   A brief explanation of the option pops up.

THIS PAGE LEFT BLANK INTENTIONALLY

# Using Norton AntiVirus

This chapter explains how to access the Norton AntiVirus main window so you can scan for viruses, set configuration options, schedule scans to run automatically, and view the Activity Log, which maintains a history of Norton AntiVirus activities.

## Tips to avoid viruses

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

- Scan all hard disk drives at least once a week to verify they are virus-free. You can schedule the scans to occur automatically.
- Scan all new files and floppy disks before first use.
- Update your virus definitions regularly to make sure you are protected against newly discovered viruses. A new definitions file is available monthly. See "Updating virus definitions" in Chapter 5 for information on how to receive the files.
- Make periodic backups of your hard disk.
- Use legal copies of all software and make write-protected backups.

## Starting and exiting Norton AntiVirus

All operations begin at the Norton AntiVirus main window.

### To start Norton AntiVirus:

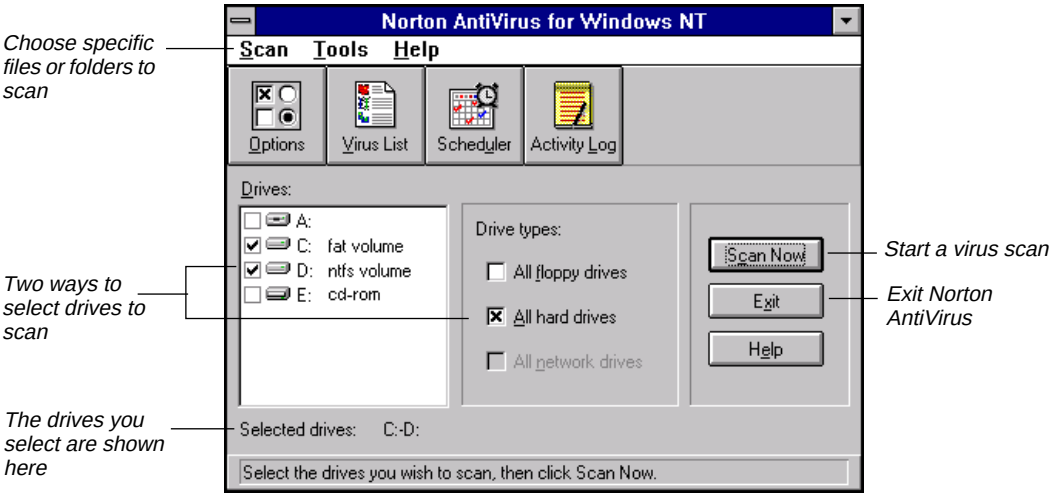

- Double click Norton AntiVirus Scanner in the Norton AntiVirus program group.

  The Norton AntiVirus main window appears (see Figure 3-1).

### To exit Norton AntiVirus:

- Click Exit in the Norton AntiVirus main window (Figure 3-1).

**Figure 3-1** Norton AntiVirus main window




# 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 Problems Found dialog box appears so you can direct repairs. After the problems are dealt with, as well as after a scan with no problems found, the Scan Summary dialog box appears detailing everything that happened.

---

**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 the scanner" in Chapter 6 for directions.

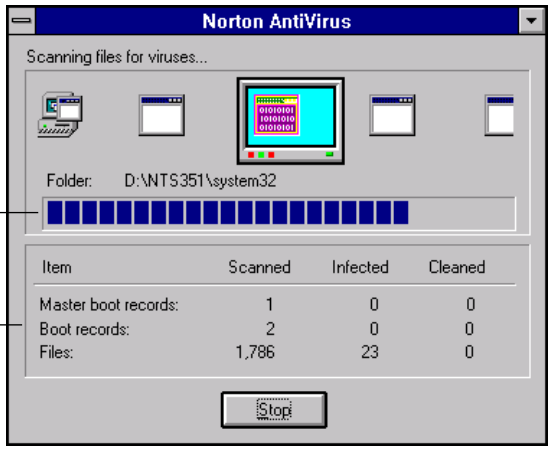
---

### To scan one or more drives:

1. Check specific drives to scan in the Drives list box or select multiple drives by checking items in the Drive Types group (see Figure 3-1).
2. Click Scan Now.

   The Scan dialog box reports the progress of the scan (Figure 3-2).

**Figure 3-2** Scan in progress




### To scan an individual file:

1. In the Norton AntiVirus main window, chooseFILE from the Scan menu.
2. Select the file you want to scan.
3. 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.

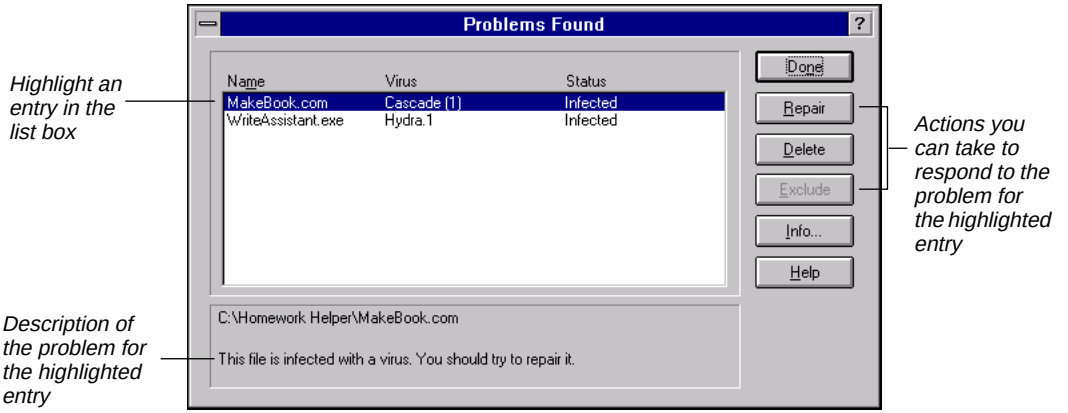
## Working with scan results

When viruses are discovered, Norton AntiVirus reports which items are infected with what viruses and presents a group of command buttons to treat each infection. If a virus is found, don't panic. Norton AntiVirus can resolve the problem. See Chapter 4, "Eliminating viruses," for detailed instructions on how to proceed.

## Problems found dialog box

The Problems Found dialog box appears at the end of the scan only if a virus is detected (Figure 3-3). It lists infected items and reports whether they are files or boot records.

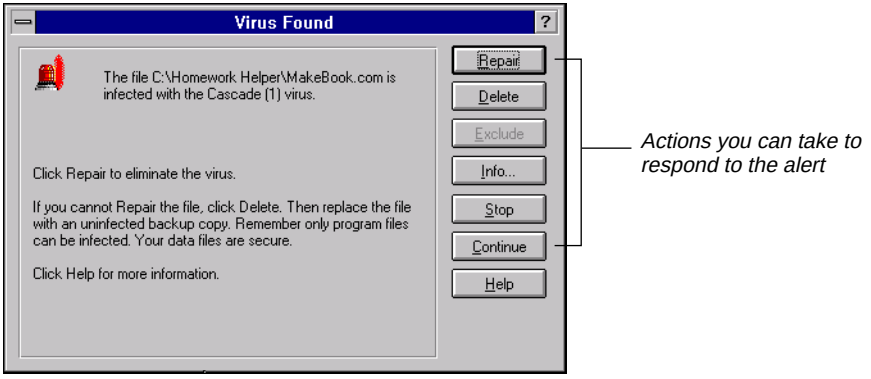
**Figure 3-3** Problems Found dialog box




## Virus alert dialog box

Some users prefer to have a virus alert generated immediately if a problem is found during a scan, rather than dealing with all problems at the end of the scan (Figure 3-4). After each virus is treated, the scan continues.

**Figure 3-4** Virus Found alert



**To generate immediate virus alerts:**

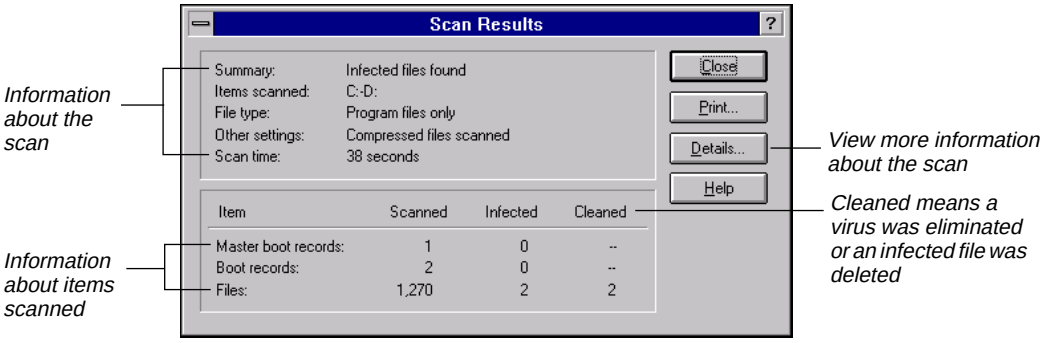
1. Click Options in the Norton AntiVirus main window.
2. Click the Scanner tab.
3. Click the Advanced button in the Scanner tab.
4. Check Immediate Notification.
5. Click OK to close the Scanner Advanced Settings dialog box.
6. Click OK to save your settings and close the Options dialog box.

See "Customizing the scanner" in Chapter 6 for detailed instructions to set other scanner options.

## Scan Results dialog box

After any problems found are addressed, or if no problems were found during the scan, the Scan Results dialog box appears. It contains summary information about the scan that was performed and the resolution of problems if any were found (Figure 3-5).

**Figure 3-5** Scan Results dialog box




From the Scan Results dialog box you can:


Click Print to send the scan results to a printer or a file.


Click Details to view more information about the scan, such as which files had problems and how each problem was resolved. If no problems were found, the Details button is dimmed.

# Selecting which files to scan

Norton AntiVirus is preset only to scan program files when you specify a drive or folder. In most situations, scanning program files is sufficient because viruses only infect and spread from these types of files. You can, however, specify that all files be scanned instead. The following sections explain file selection for scanning so you can decide which setting is best for your situation.

## All files

Scans every file—data files (such as databases, documents, text files, and spreadsheets) and program files (such as system files, word processing programs, and utility programs). Although it is rare, viruses can infect and damage data files. Scanning all files takes longer, but includes any executable files 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

Scans files with extensions contained in the Norton AntiVirus Program File Extensions list. This list contains the most common extensions for executable files, which are most likely to become infected and spread viruses. See "Specifying program file extensions" in Chapter 6 for detailed information about the extensions list and how to modify it. Remember, scanning only program files is sufficient in most cases.

---

**NOTE:** The extensions for Microsoft Word documents are included in the program files group. Although these are not program files, they can be infected by a new 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 do this, 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.

### To select all files or program files only for scanning:

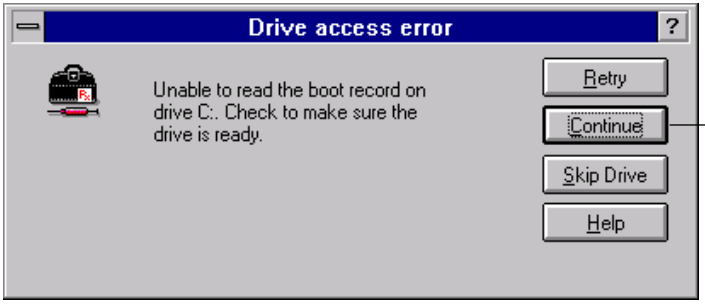
1. Click Options in the Norton AntiVirus main window.
2. Click the Scanner tab.
3. In the What to Scan group box, click one of the following options:
   - All Files: Scans all files in the specified folder or drive. This includes files less susceptible to viruses.
   - Program Files: Scans files that are most likely to become infected. Only the files with an extension that is specified in the Program File Extensions list are scanned.
4. Click OK to close the dialog box.

## Bypassing boot record scans

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

As a security precaution, some Windows NT systems are configured to prevent users from accessing these disk areas. You must have administrator-level privileges to scan boot records. If you see a dialog box saying that you cannot access the boot records, you can set a configuration option to bypass boot record scans (Figure 3-6).

**Figure 3-6** Access to boot records denied




### To bypass boot record scans:

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

3 Uncheck the first two items in the What to Scan group box:
   - Master Boot Record
   - Boot Records
4 Click OK to save your settings and close the dialog box.


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

See "Customizing the scanner" in Chapter 6 for detailed instructions to set other scanner options.

# Scheduling virus scans

You can schedule a weekly virus scan that runs unattended. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working at the computer.

**NOTE:** You must have administrator-level rights to schedule scans.

### To schedule automatic scans:

1 Click Scheduler in the Norton AntiVirus main window.

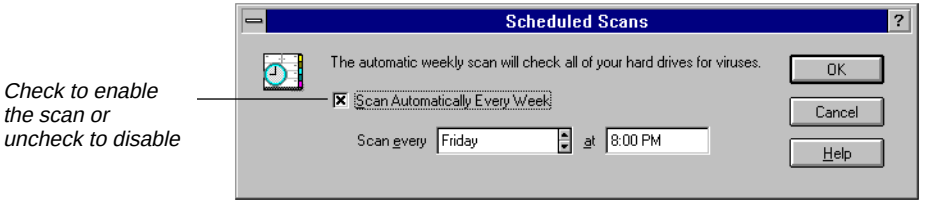
The Scheduled Scans dialog box appears (Figure 3-7).

2 Check Scan Automatically Every Week.

Uncheck this option if you want to disable the automatic scans.

3 Specify the day of the week and the time for the scan.

**Figure 3-7** Scheduled Scans dialog box




4 Click OK to save your settings and close the dialog box.

**TIP:** From a command prompt, you can use the AT command to schedule multiple scans under Windows NT. See "Using command-line switches" later in this chapter for instructions on running the scanner (N32SCANW) directly from the command line.

# Viewing the Activity Log

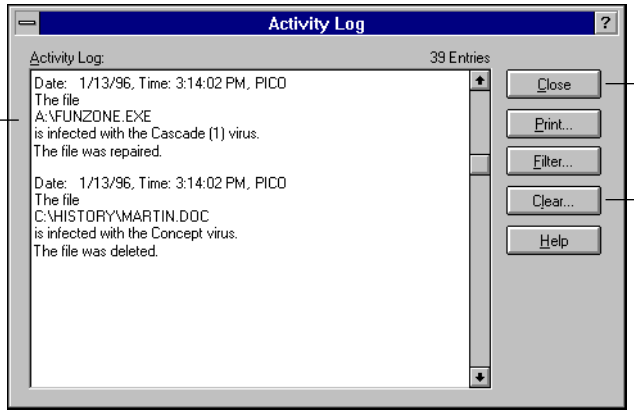
The Activity Log file contains details of Norton AntiVirus activities, such as when problems were found and how they were resolved. For directions to specify what is stored in the Activity Log, see "Customizing the Activity Log" in Chapter 6.

### To view all entries in the Activity Log:

1 Click Activity Log in the Norton AntiVirus main window.

The Activity Log appears (Figure 3-8).

**Figure 3-8** Activity Log




2 Click Close to exit the Activity Log.

### From the Activity Log dialog box you can also:


Click Print to send the Activity Log to a printer or a file.

**TIP:** Only the entries currently displayed in the list box are printed. If you filter the Activity Log, only the filtered entries are printed.


Click Filter to display specific types of events, such as all virus detections. See the next section, "Filtering Activity Log entries," for more information.


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

## Filtering Activity Log entries

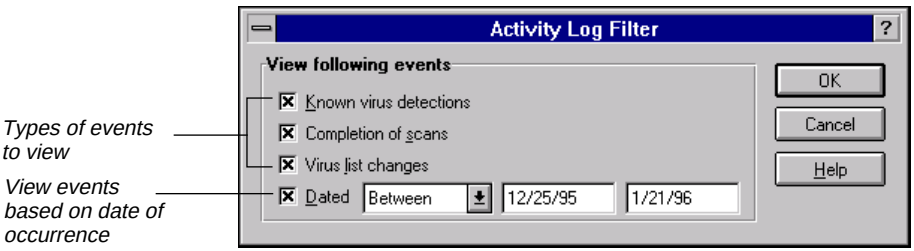
You can filter the Activity Log to display specific categories of entries, such as virus detections only.

### To filter the Activity Log entries:

1 Click Filter in the Activity Log dialog box (see Figure 3-8).

The Activity Log Filter dialog box appears (Figure 3-9).

**Figure 3-9** Activity Log Filter dialog box




2 Check the types of events you want listed. If no entries match your filter, a No Items to Display dialog box appears instead.

- Known Virus Detections: Displays information on known virus detections.
- Completion of Scans: Displays information about when scans occurred.
- Virus List Changes: Displays information about changes to the virus list.
- Dated: Indicates the date or range of dates for displaying the selected events. Select an option in the Date drop-down list box, then enter the date or dates to define the range.

3 Click OK.

# Using command-line switches

N32SCANW.EXE is the Windows NT interface and scanner. It can be run with command-line switches to override configuration settings. When scanning using command-line switches, Norton AntiVirus runs minimized, but will pop open on your screen if a virus is found.

Some switches are used alone, while others are followed by a parameter, either a plus (+) or minus (-) sign. You can use more than one switch and more than one parameter on a command line. The vertical bar symbol (|) means that you should use either parameter, but not both. Do not type the brackets around the parameters on the command line. Use the following syntax to run N32SCANW with switches:

```
N32SCANW [pathname] [options]
```

| | |
|---|---|
| `pathname` | Any drive, folder, file, or combination of these is scanned. To scan multiple items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files; for example, N32SCANW 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 (see "Setting advanced options" in Chapter 6). |
| `/L` | All local drives, except drives A: and B:, are scanned. |
| `/S[+\|-]` | Enables (+) or disables (-) scanning of subfolders for any folders specified in the pathname. S+ is the default. |
| `/B[+\|-]` | Enables (+) or disables (-) scanning of boot records; for example, N32SCANW A: /B+ or N32SCANW A: /B- (default is the Scanner options setting). |
| `/BOOT` | Only the boot records of the specified drives are scanned. |

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

- To scan all .EXE files in your WIN32APP folder and descending subfolders, type the following:

  ```
  N32SCANW C:\WIN32APP\*.EXE
  ```

- To scan all .EXE files in your WIN32APP folder only:

  ```
  N32SCANW C:\WIN32APP\*.EXE /S-
  ```

- To scan a folder and descending subfolders with long filenames (LFN), use double quotes:

  ```
  N32SCANW "C:\Program Files"
  ```

- To scan a drive and a folder on another drive:

  ```
  N32SCANW C: D:\DOWNLOAD
  ```

- To scan a folder on the network drive P: called PROGRAMS but none of its subfolders:

  ```
  N32SCANW P:\PROGRAMS /S-
  ```

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

  ```
  N32SCANW C: A: /BOOT
  ```

- To use the Windows NT Scheduler Service to initiate an automatic scan of all local drives (except the A: and B: drives) at 5:30 P.M. every weekday, enter the following command on one line:

  ```
  at 17:30 /interactive /every:M,T,W,Th,F
  "c:\win32app\navnt\n32scanw" /L
  ```

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

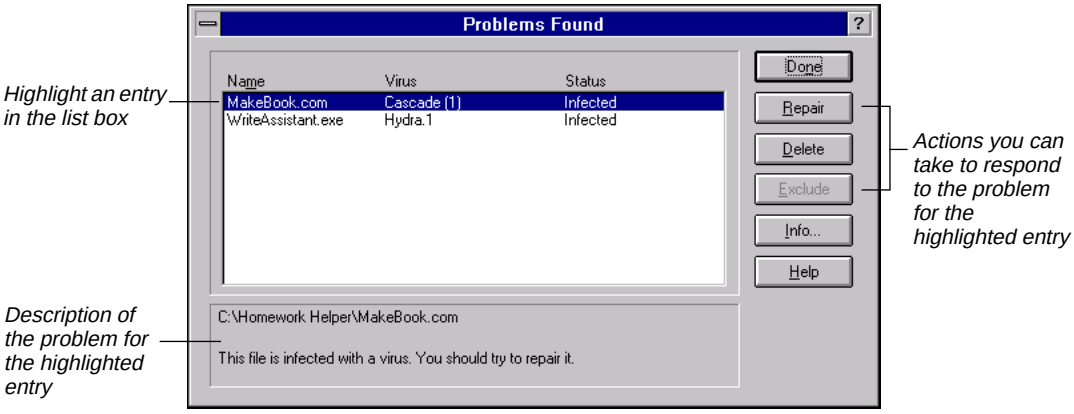
# Eliminating viruses

This chapter explains how Norton AntiVirus warns you of a possible computer virus and how you should respond.

## Problems found

Norton AntiVirus displays a Problems Found dialog box at the end of a scan only if a virus is detected. Figure 4-1 shows an example Problems Found dialog box.

**Figure 4-1** Problems Found dialog box




**TIP:** Some users prefer to have a virus alert generated immediately if a problem is found during a scan, rather than dealing with all problems at the end of the scan. If you want an alert generated immediately rather than the Problems Found dialog box at the end of the scan, check Immediate Notification when setting Scanner Advanced options. See "Setting advanced options" in Chapter 6 for directions.

## What to do next

Don't panic! If a virus is found, Norton AntiVirus can remove it from your computer. Simply follow the instructions in this section.


**WARNING:** If you have any open DOS sessions, close them all immediately and scan again. A virus may be active in the memory space of a DOS session and continue to infect and damage files. Closing the DOS sessions removes any active viruses from memory.

### If problems are listed in the Problems Found dialog box:

1. Highlight an entry in the list box.
2. 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.
3. See Table 4-1 for information about the command buttons in the Problems Found dialog box, then click the appropriate button.

### If a Virus Found alert appears on your screen:

1. Read the message in the alert box to understand the type of problem that was found.
2. See Table 4-1 for information about the command buttons in the alert box, then click the appropriate button.

Later sections in this chapter discuss the problems and alerts in more detail. If the message on your screen is not discussed in this chapter, see Appendix A, "System messages," for more information.

Some buttons that are displayed in a Problems Found or Virus Found dialog box may be dimmed. They are unavailable for one of two reasons:

- Option is not permitted for your particular Norton AntiVirus configuration. These options are set on the Scanner tab.

  See "Customizing the scanner" in Chapter 6 for information on changing the preset options.
- Norton AntiVirus has determined that a particular action cannot be performed in the current situation.

**Table 4-1** Command buttons to respond to viruses

| Button | Result | Additional Information |
|---|---|---|
| Repair | Eliminates the virus and returns the infected file or boot record to its original state. | See "Responding to problems found or virus alerts" later in this chapter. |
| Delete | Eliminates the virus by deleting the infected file. | Deleted files cannot be recovered.<br>After the file is deleted, replace it with an uninfected copy. |
| Continue | Continues the current operation. | Selecting Continue does not solve the problem that was reported. Norton AntiVirus will notify you again during the next scan. |
| Exclude | Continues the operation and excludes the file for notifications 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.<br>See "Managing exclusions" in Chapter 6 for more information. |
| Info... | Displays detailed information about the virus that was found. | See "Viewing the virus list" in Chapter 5 for more information. |

# Responding to problems found or virus alerts

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

- Repair the infected file, boot record, or master boot record.
- Delete the infected file from the disk.

  You cannot, however, delete infected in-use files, boot records, or master boot records. See the next section, "What to do if repair is unsuccessful," for instructions on how to proceed if a repair cannot be made or a file cannot be deleted.


**WARNING:** Files deleted by Norton AntiVirus cannot be recovered.

### To repair an infected file or boot record:


1. Do one of the following, depending on your Norton AntiVirus configuration:
   - Highlight the item in the Problems Found dialog box and click Repair.
   - Click Repair in the Virus Alert dialog box.

   If the Repair command button is dimmed, 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 again. This verifies that there aren't any other files or boot records that contain viruses.

**TIP:** Norton AntiVirus is preset to make backup copies of files before they are repaired. The backup files have a "VIR" extension. These backup files are not scanned in the future. Be sure to delete them once you know the repair was successful. For more information, see "Setting backup options" in Chapter 6.

### To delete an infected file:


1. Do one of the following, depending on your Norton AntiVirus configuration:
   - Highlight the item in the Problems Found dialog box and click Delete, then follow the prompts on your screen.
   - Click Delete in the Virus Alert dialog box, then follow the prompts on your screen.

   If the Delete command button is dimmed, 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 again 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 more information, see "Viewing the Activity Log" in Chapter 3.

Although an infected file within a compressed file will be detected during scans, Norton AntiVirus cannot repair the file in its compressed state.

**To remove viruses from infected compressed files:**

1. Create a temporary folder.
2. Decompress the compressed file into the temporary folder.
3. Delete the infected compressed file.
4. Scan the temporary folder and repair or delete any infected files.
5. Recompress the files in the temporary folder, if desired.

# What to do if repair is unsuccessful

In the rare instance when Norton AntiVirus is not able to repair a file or boot record, the following two messages notify you that the repair was not successful. See Appendix B, "Emergency recovery," for additional information on getting help for any virus emergency.

## Unable to repair a file

If Norton AntiVirus cannot repair the infected file, the only way to remove the virus is to delete the file. After you delete the infected file, you can replace it with an uninfected copy.

If the infected file is a system file that is in use or otherwise required for operation, you must perform a manual repair. During Windows NT installation, you created an Emergency Repair Disk. Try using this disk to restore the damaged system file. If this too fails, you must reinstall Windows NT from your original installation disks. As a safety precaution, first back up your data files and uninfected program files.

## Unable to repair a boot record

You must have administrator-level privileges to access boot records. If you have the proper privileges and cannot effect a repair, Windows NT itself may be preventing the boot record modifications. For example, FAT volumes that are in use cannot be repaired. In this case, use the Norton AntiVirus Scanner for DOS, a free program provided by Symantec that runs under MS-DOS rather than Windows NT, to repair boot records. See Appendix B, "Emergency recovery," for information on how to get the program. The text file that accompanies the program gives detailed procedures for its use.

If you don't succeed with the DOS scanner, use the Emergency Repair Disk that you created during Windows NT installation to restore the boot records.

If this too fails, you must reinstall Windows NT from your original installation disks.

Again, as a safety precaution, first back up your files. In all cases, never boot from the infected system before attemping a repair.

**TIP:** If Norton AntiVirus cannot successfully repair a boot record on a floppy disk, you can often copy important files from the floppy disk to another disk. But be careful—the floppy disk is still infected. Scan all files you copy from the floppy disk for viruses again. After you've copied all important files from the infected floppy disk, either discard the disk or reformat it. From a command prompt, use FORMAT A: /U for an "unconditional format." From Program Manager, don't use the Quick Format option.

# Dealing with common problems

This section explains how to resolve some common problems that may arise while you are using Norton AntiVirus. Follow the suggestions provided here to try to solve these problems before calling for technical support.

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

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

Solution: Scan all floppy disks. See "Scanning for viruses" in Chapter 3 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" in Chapter 3 and "Specifying program file extensions" in Chapter 6 for information on how to change the selection of files for scanning.

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

Solution: Close all open DOS sessions and scan again.

## A program does not work properly after repair

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

Solution: Replace the program with an uninfected original.

THIS PAGE LEFT BLANK INTENTIONALLY

# Keeping up with new viruses

This chapter explains how to update virus definitions files and view details about the viruses that Norton AntiVirus detects.

## Updating virus definitions

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

### Virus definitions update sources

Updated virus definitions files provided by Symantec are available from a variety of sources. Choose the one most convenient for you.

#### CompuServe

The current virus definition files are in the Symantec Forum.

**To directly access the Symantec Forum:**

1. Do one of the following:
   - Choose GO from the Services menu and enter `SYMNEW`
   - At any ! prompt, type `GO SYMNEW`
2. The files are located in the Norton AntiVirus library.

#### America Online

**To access the Symantec bulletin board:**

1. Choose KEYWORD from the GoTo menu.
2. Type `SYMANTEC`
3. Click Software Libraries.

4. Click Windows NT Products.
5. Follow the on-screen directions.

## Internet

The virus definitions files are located in the Symantec File Transfer Protocol (FTP) Internet site.

**To use the FTP site:**

1. Access `ftp://ftp.symantec.com`
2. The files are located in the `/public/win95_nt/nav/` directory.

**To use the World Wide Web site:**

1. Access `http://www.symantec.com`
2. Click AntiVirus Reference Center.
3. Click NAV.
4. Follow the on-screen directions.

## Microsoft Network

**To access the Symantec service:**

1. Choose Go To from the View menu.
2. Type `SYMANTEC`
3. Double click Support Solutions.
4. Double click Norton AntiVirus 95 (the same files are used for Windows NT).
5. The virus definitions are located in the File Library.

## Symantec BBS

**Settings for the Symantec BBS are:**

- 8 data bits, 1 stop bit, no parity

**To contact the Symantec BBS, use one of the following telephone numbers:**

- 300- to 28,800-baud modems (541) 484-6669 (24 hrs.)
- 300- to 14,400-baud modems (541) 984-5366 (24 hrs.)

**To access definitions from the main menu of the Symantec BBS:**

1. Press `F` to get a file.
2. Press `N` to get the latest NAV definitions.
3. Follow the on-screen directions to download the file.

**To go directly to the file library:**

1. As soon as you log in, type `/GO NAVNT`
2. Follow the on-screen directions to download the file.

### Virus definitions update disks

You can order virus definitions update disks from Symantec to arrive by mail. This service requires a fee.

**To order, do one of the following:**

- In the United States, call (800) 203-4403.
- Outside the United States, contact your local Symantec office or representative.

## Installing new virus definitions files

The virus definitions file you download is a compressed archive that contains several files. Its name, which changes from month to month, uses the following form: *mm*NAV*yy*.ZIP, where *mm* is the month and *yy* is the year.

The actual definitions files can be extracted from the archive using several different utilities. The following procedure uses PKUNZIP.

**To install the new virus definitions:**

1. From a command prompt, copy the downloaded compressed file to your Norton AntiVirus folder. C:\WIN32APP\NAVNT is the default location.
2. Use the PKUNZIP utility to extract the files from the compressed file; for example:

   ```
   PKUNZIP 01NAV96.ZIP
   ```

   When prompted to Overwrite, press “y” for yes. You’re replacing your existing files with the new ones.
3. After all the files are extracted successfully, delete the compressed file.

4 Initiate a scan with Norton AntiVirus to activate the new virus definitions.

5 Read the text files (*.TXT) for late-breaking news about newly discovered viruses and any special precautions that you should take.

If you don't have a copy of PKUNZIP, the utility that extracts the compressed files, it is available for download at both the Symantec Internet site and BBS. The file, called "PKZ204G.EXE," is a self-extracting archive. Just run the downloaded file to get PKUNZIP.

The utility is also available from the other online services. Perform a file search for PKZIP or PKUNZIP to locate the proper library.

# Viewing the Virus List

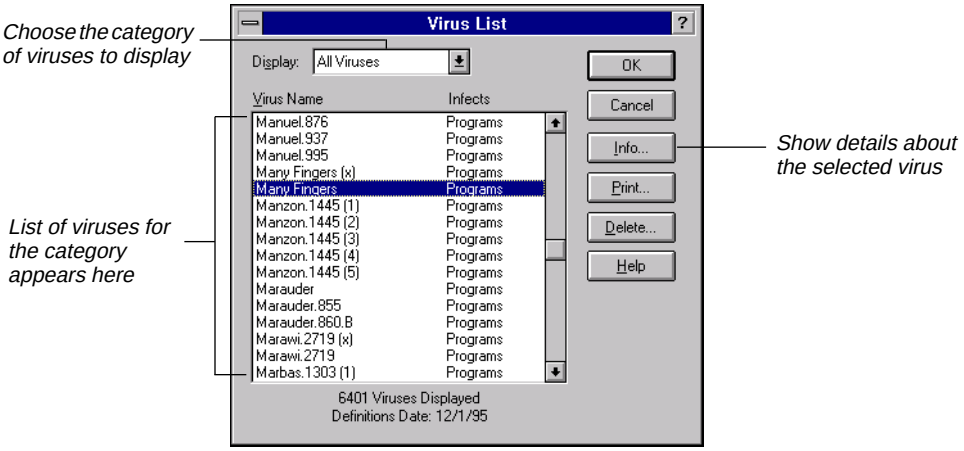
You can see which viruses Norton AntiVirus detects by viewing the list of virus names. You can also view descriptions of particular viruses, including their symptoms and aliases.

### To view the list of virus names:

- Click Virus List in the Norton AntiVirus main window.

  The Virus List appears (Figure 5-1).

**Figure 5-1** Virus List




The list box displays the name of the virus and what it infects (program files, boot records, or both). You can view different categories of viruses by selecting a category from the Display drop-down list box.

| | |
|---|---|
| **All Viruses** | All viruses that Norton AntiVirus can detect. |
| **Common Viruses** | Only the most common viruses. These are viruses you are most likely to encounter. |
| **Program Viruses** | Only viruses that can infect program files. |
| **Boot Viruses** | Only viruses that can infect boot records or master boot records on disks. |
| **Stealth Viruses** | Viruses that try to conceal themselves from attempts to detect or remove them. |
| **Polymorphic Viruses** | Viruses that appear differently in each infected file. |
| **Multipartite Viruses** | Viruses that can infect both program files and boot records. |


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

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

Click Delete to delete the currently highlighted definition.


**WARNING:** Do not delete a virus definition unless you are sure you don't need it anymore. Once a virus definition is deleted, files and boot records are no longer protected from that virus until you update the virus definition files again.

### To search for a virus name:

1. Activate the Virus List by clicking inside the list box (see Figure 5-1).
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.

THIS PAGE LEFT BLANK INTENTIONALLY

# Customizing Norton AntiVirus

This chapter explains how to customize Norton AntiVirus. Generally, you do not need to change any settings. The preset (or default) options give appropriate virus protection for most users.

## Customizing the scanner

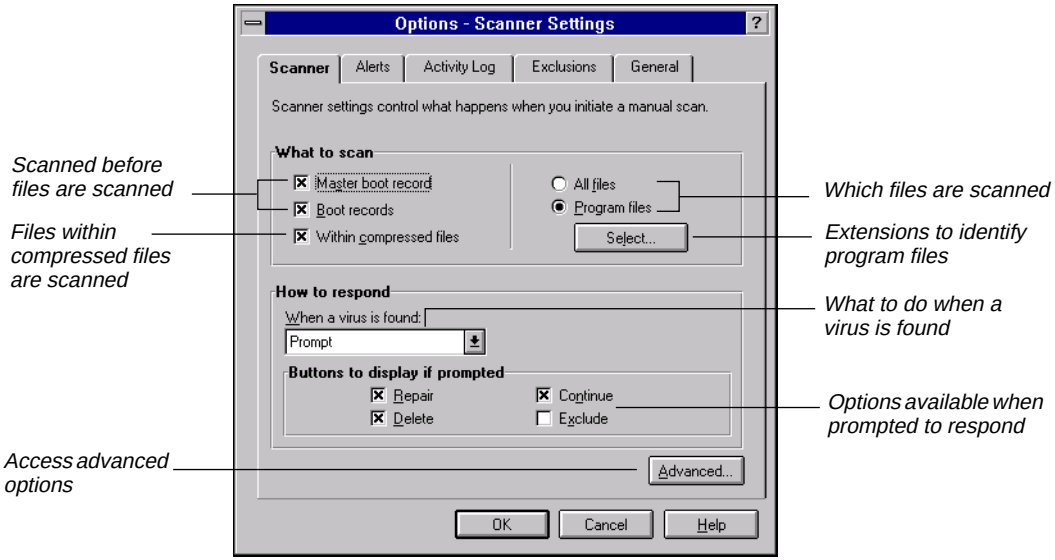
The Scanner options affect scans you initiate when you click the Scan Now button or when scheduled scans occur. The options settings let you:

- Specify what is scanned.
- Determine what happens if a virus is detected.
- Set advanced options, including whether to display the Problems Found dialog box at the end of a scan or a Virus Found alert immediately.

### To customize what to scan:

1. Click Options in the Norton AntiVirus main window.
2. Click the Scanner tab (Figure 6-1).

**Figure 6-1** Scanner Settings tab



3 Select which areas of your computer Norton AntiVirus should scan before files are scanned in the What to Scan group box.

- 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 the PKZIP or LHARC utilities (ZIP and LHA). Scanning time may increase slightly if you have many compressed files. Note that compressed files within compressed files are not scanned.

4 Specify the types of files to scan in the What to Scan group box:

- All Files: Scans all files in the specified folder or drive. This includes 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, see "Selecting which files to scan" in Chapter 3. For information on the extensions list, see "Specifying program file extensions" later in this chapter.

5 Click OK to close the dialog box.

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

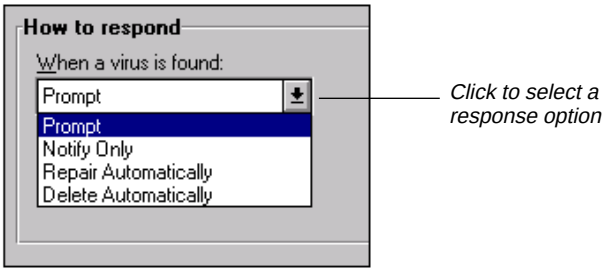
### To customize how to respond when a virus is found:

1 Click Options in the Norton AntiVirus main window.

2 Click the Scanner tab (see Figure 6-1).

3 Select an option in the How to Respond drop-down list box (Figure 6-2).

**Figure 6-2** How to Respond 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.
- 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.

  Note that Norton AntiVirus is preset to make backup copies of files before they are repaired. For more information, see "Setting backup options" later in this chapter.
- 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.


**WARNING:** Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be recovered.

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.
- Continue: Allows you to continue scanning without resolving the problem. The Continue button applies only when Immediate

Notification is turned on (see the next section, "Setting advanced options," for details on the Immediate Notification option).

- 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.

## Setting advanced options

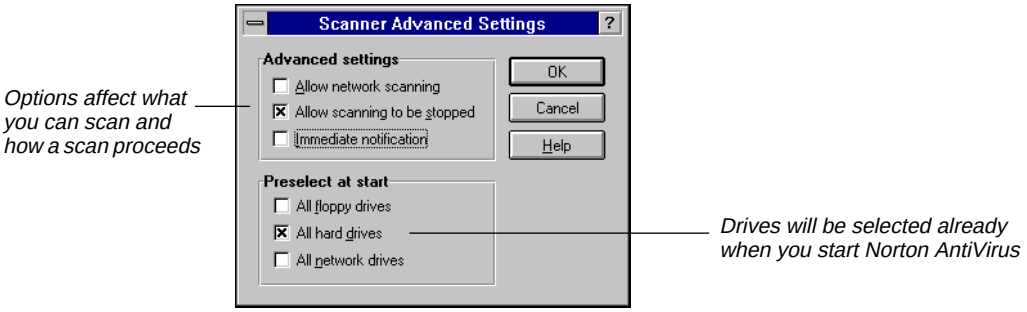
The scanner advanced settings affect what you can scan and how a scan proceeds.

### To set additional scanning options:

1 Click the Advanced button in the Scanner tab (see Figure 6-1).

The Scanner Advanced Settings dialog box appears (Figure 6-3).

**Figure 6-3** Scanner Advanced Settings dialog box




2 Check the Advanced Settings options that you want to enable:

- Allow Network Scanning: Allows you to scan network drives.
- Allow Scanning to be Stopped: Allows you to halt a scan in progress. When this option is checked, the Stop button is available during a scan.
- Immediate Notification: Displays an alert box when a problem is detected while scanning. This allows you to respond immediately, instead of waiting until the scan is completed.

3 In the Preselect at Start group box, specify the drives that you want selected automatically in the Drives list box when you start Norton AntiVirus.

4 Click OK to save your settings and close the dialog box.

# Specifying program file extensions

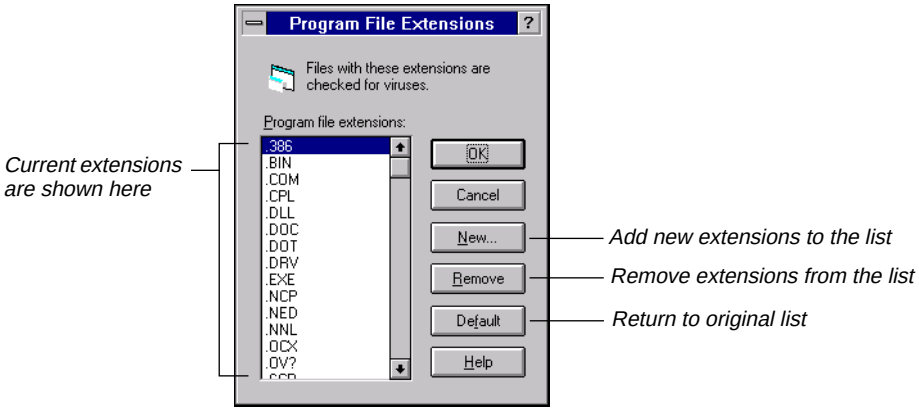
Norton AntiVirus uses the Program File Extensions list when scanning program files. The list contains the file extensions for files most likely to become infected and spread viruses. If you are using custom applications that use unique file extensions, add them to the list. File extensions are always three characters.

### To view the current program file extensions:

1. Select the Program Files option in the Scanner tab (see Figure 6-1).
2. Click Select.

   The Program File Extensions dialog box appears (Figure 6-4).

**Figure 6-4** Program File Extensions dialog box



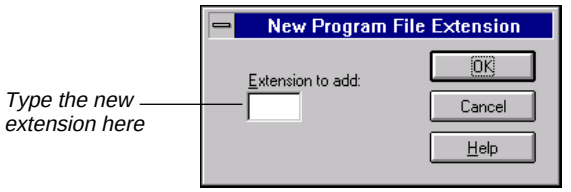

**NOTE:** Microsoft Word documents are included in the program files group. Although these are not program files, they can be infected by a new class of viruses called "Macro viruses."

### To add a program file extension:

1. Click New in the Program File Extensions dialog box (see Figure 6-4).

   The New Program File Extension dialog box appears (Figure 6-5).

**Figure 6-5** New Program File Extension dialog box




2 Type the new file extension in the Extension to Add text box.

You can use wildcards in the extension, but not to represent all three characters. For example, .OV? represents files with extensions that begin with .OV, such as .OVL and .OV1.

3 Click OK.

### To remove a program file extension:

1 Select the file extension in the Program File Extensions dialog box (see Figure 6-4).

2 Click Remove.

3 Click OK.

### To reset the list of program file extensions:

1 Click Default in the Program File Extensions dialog box (see Figure 6-4).

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

2 Click OK.

## Setting backup options

As a safety precaution, Norton AntiVirus is preset to make a backup copy of a file before it attempts a virus repair. The default extension is ".VIR" for virus-infected, backed-up files. You can use a different extension, if desired, or choose not to have these backups made at all.

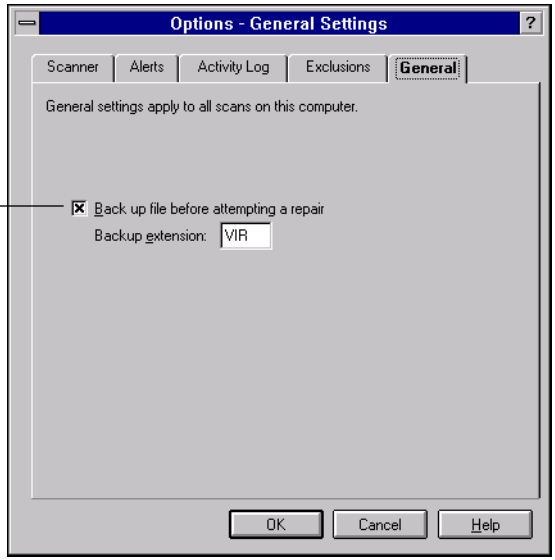
All files with the backup extension are added automatically to the Exclusions List so they will not be reported again during a scan. See the next section, "Managing exclusions," for more information.

Delete these backup files after you determine that the repair operation is successful. Even though the infected backup files can't be run (because of the .VIR file extension)—they contain viruses!

**To change backup settings:**

1. Click Options in the Norton AntiVirus main window.
2. Click the General tab (Figure 6-6).

**Figure 6-6** General Settings tab




*Makes a back up copy of the virus-infected file*

3. Check Back Up File Before Attempting a Repair to have Norton AntiVirus make a copy of the infected file before repairing it.
4. If desired, enter a different file extension in the text box.
5. Click OK.

# Managing exclusions

Norton AntiVirus utilizes the entries in the Exclusions List in all scans. You assign exclusions to *items*—drives, folders, groups of files, or single files. Any item in the list is not scanned for viruses. If you move or rename a file, you automatically invalidate its exclusion.

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

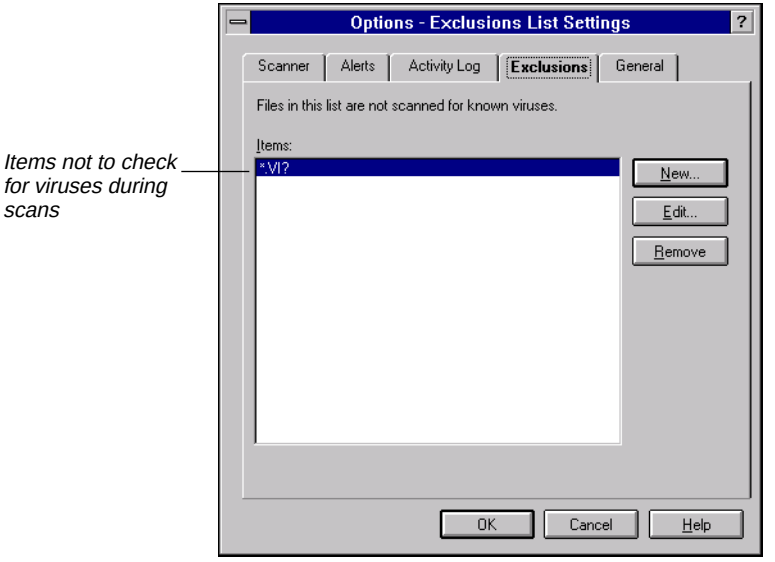
In practice, items are added to the Exclusions List when you click the Exclude button in the Problems Found dialog box at the end of a scan or in a Virus Found alert to resolve a virus event that Norton AntiVirus detected but you deem acceptable.


**WARNING:** Unless you have a specific reason for excluding something from a scan, don't modify the default list. It specifies only the virus-infected backup files that Norton AntiVirus creates before a repair (see "Setting backup options" earlier in this chapter). If you set an exclusion, a virus can creep in.

### To view the Exclusions List:

1. Click Options in the Norton AntiVirus main window.
2. Click the Exclusions tab (Figure 6-7).

**Figure 6-7** Exclusions List Settings tab

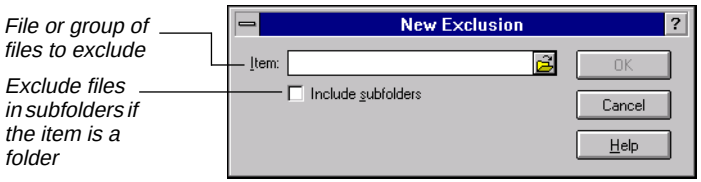



### To add exclusions manually:

1. Click New in the Exclusions tab (see Figure 6-7).

   The New Exclusion dialog box appears (Figure 6-8).

**Figure 6-8** New Exclusion dialog box




2 Type the pathname for the file or group of files in the Item text box.

3 Check Include Subfolders if you want files in descending folders of the item to be excluded also.

4 Click OK.

### To remove an exclusion:

1 Select a file or group of files from the Items list box in the Exclusions tab (see Figure 6-7).

2 Click Remove.

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

3 Click OK.

### To modify an existing exclusion:

1 Select a file or group of files from the Items list box in the Exclusions tab (see Figure 6-7).

2 Click Edit and make the desired changes.

3 Click OK.

## Customizing the Activity Log

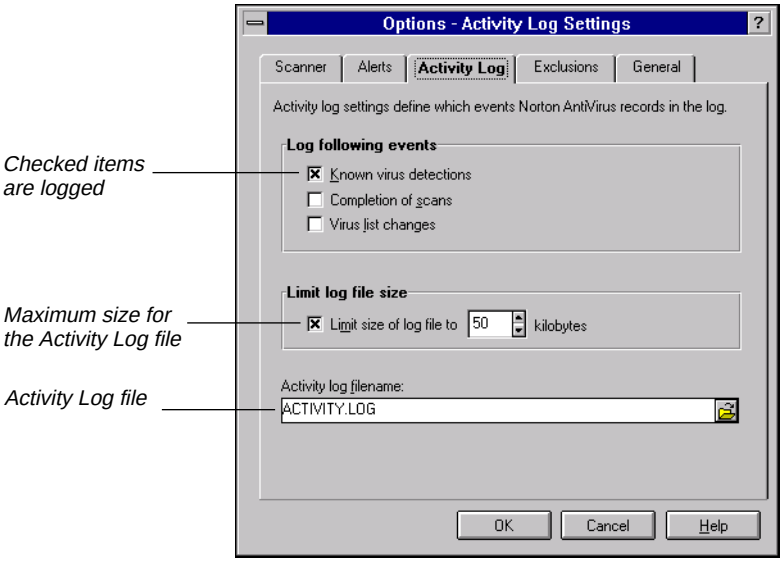
The Activity Log contains a history of Norton AntiVirus activity. For example, Norton AntiVirus is preset to record detections of known viruses and what action was taken on infected files (whether they were repaired, deleted, added to the Exclusions List, or left untouched).

### To customize the Activity Log:

1 Click Options in the Norton AntiVirus main window.

2 Click the Activity Log tab (Figure 6-9).

**Figure 6-9** Activity Log Settings tab




3 In the Log Following Events group box, check each type of event that you want Norton AntiVirus to record:

- Known Virus Detections: Records detections of known viruses (viruses identified in the Virus List).
- Completion of Scans: Records the date and ending time of scans that you initiate and scheduled scans.
- Virus List Changes: Records changes to the Virus List.

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

When the specified file size is reached, each new entry added to the activity log causes the oldest entry or entries to be deleted.

5 Enter the pathname for the Activity Log file in the Activity Log Filename text box.

6 Click OK to save your settings and close the dialog box.

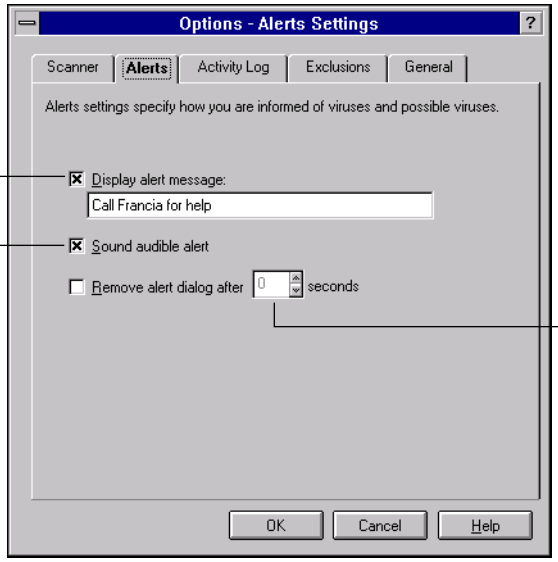
# Customizing alerts

The alert settings define how Norton AntiVirus informs you that it has detected a virus if you choose to have Virus Found alerts generated immediately rather than use the Problems Found dialog box at the end of a scan. See "Setting advanced options" earlier in this chapter for instructions.

### To customize alerts:

1. Click Options in the Norton AntiVirus main window.
2. Click the Alerts tab (Figure 6-10).

**Figure 6-10** Alerts Settings tab




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 (up to 76 characters) 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.

   If you configure Norton AntiVirus for Immediate Notification (see "Setting advanced options" earlier in this chapter) and choose Repair or

Delete Automatically when a virus is found (see "Customizing the scanner" earlier in this chapter), these actions will take place when the set time expires.

6 Click OK.

# System messages

This appendix contains a list of the error messages you may see while using Norton AntiVirus. The messages are listed in alphabetical order.

Note that whenever an item such as <FILENAME>, <DRIVE>, or <VIRUS NAME> appears, it is replaced by an actual filename, drive letter, drive number, or virus name in the message on your screen.

## Messages and their meanings

### 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 problems found or virus alerts" in Chapter 4.

### 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 problems found or virus alerts" in Chapter 4.

### 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 problems found or virus alerts" in Chapter 4.

### 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 problems found or virus alerts" in Chapter 4 for more information.

### The master boot record of hard 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 problems found or virus alerts" in Chapter 4.

### Unable to access drive: <DRIVE>.

Norton AntiVirus could not access the specified drive because you do not have access privileges to the drive, the drive door is open, or there is a problem with the drive.

### Unable to complete scan.

Norton AntiVirus found more problems than can be reported at one time. Correct the problems reported, then scan again. Norton AntiVirus will report any additional problems it finds. See Chapter 4, "Eliminating viruses," 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 "Updating virus definitions" in Chapter 5 for information on getting updated virus definitions files.

### Unable to print the requested information.

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

### 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 problems found or virus alerts" in Chapter 4 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 Appendix B, "Emergency recovery," for information.

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

Norton AntiVirus was not able to repair the master boot record on the specified drive. See Appendix B, "Emergency recovery," for 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 the 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.

THIS PAGE LEFT BLANK INTENTIONALLY

# Emergency recovery

This appendix explains what to do in a virus emergency.

## Virus hotline

The Norton AntiVirus group of Symantec Corporation, as part of its continuing commitment to halt the spread of computer viruses, has set up a special telephone hotline to help you recover from any virus emergency—regardless of which anitivirus software you may use. To get help, or just answers to virus questions, call the following telephone number:

(541) 9VIRUS9

(541) 984-7879

Technicians are available to take your calls from 7:00 A.M. until 4:00 P.M. (Pacific Daylight Time), Monday through Friday, excluding holidays.

## When you can't start your computer

Boot sector viruses sometimes prevent you from starting up your computer at all. You won't be able to use the Norton AntiVirus Scanner for Windows NT to diagnose and repair the problem.

To help in this situation, Symantec provides a free MS-DOS based scanner. The Norton AntiVirus Scanner for DOS (NAVSCAN.EXE) is available to download from all of the on-line services described in Chapter 5, "Keeping up with new viruses."

---

**TIP:** As a precaution, download NAVSCAN when you next update your virus definitions.

---

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

THIS PAGE LEFT BLANK INTENTIONALLY

# Glossary

**access priveleges** — Windows NT security permissions for files, folders, and objects.

**application** — *See* program.

**(to) boot** — To start the computer.

**bootable disk** — A disk that contains the operating system necessary to start, or boot, the computer.

**boot record** — The first physical sector on a floppy disk or the first logical sector of a hard disk partition. It identifies the disk's architecture (sector size, cluster size, and so on). It also contains the boot record program.

**boot record program** — The program that is responsible for loading the operating system.

**boot virus** — A virus that infects the boot record program on both hard and floppy disks and/or the master boot record program on hard disks. A boot virus loads into memory before the operating system, taking control of your computer and infecting any floppy disks that you access.

**bulletin board system (BBS)** — An online service that allows messaging, electronic mail, and file transfer between computer users via modem.

**cold boot** — To 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.

**.COM file** — *See* executable file.

**command-line switch** — An option that controls the operation of a program.

**compressed file** — A single file or series of files that have been compressed into one file using a utility such as PKZIP or LHARC.

**data file** A file that is created by or associated with an application and contains no executable code. Examples include word processing documents, databases, and spreadsheets (.DBF, .DAT, .WKS, etc.). *See also* macro virus.

**directory** *See* folder.

**download** To transfer a file from one computer system to another through a modem. Most frequently used when referring to the act of transferring a file from a bulletin board system.

**dropper** A program that installs a virus on your computer. Droppers are not viruses, they are trojan horse programs. *See also* trojan horse.

**exclusion** An item that you have instructed Norton AntiVirus to ignore during a scan.

**.EXE file** *See* executable file.

**executable file** A file containing a program that can be launched. Executable files generally have the following extensions: .COM, .EXE, .OVR, .OVL, .DRV, .BIN, or .SYS.

**folder** A portion of a disk that you designate to store information about files. Folders make it easier for you to organize the files on your disk. Also called a directory.

**infected file** A file that contains a virus.

**known virus** Any virus that Norton AntiVirus can detect and identify by name.

**.LHA file** A series of files that have been compressed into one file (usually with a .LHA file extension) using LHARC.

**macro virus** A 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)** The first physical sector on a hard disk. It contains the master boot record program and information on how a hard disk is partitioned.

**master boot record program** — The program that is responsible for directing the computer to load the boot record program from the bootable hard disk.

**multipartite virus** — A virus that infects and spreads from both program files and boot records.

**network** — Computers and associated hardware (printers and so forth) connected together in a work group for the purpose of sharing information and hardware among users.

**NTFS** — The Windows NT File System, which supports numerous security features. *See also* access privileges.

**operating system** — The master control program that is loaded into memory when you start up or boot your computer. It controls and manages all computer operations and programs.

**partition table** — A table in the master boot record of a hard disk that specifies how the disk is set up, such as the size and location of the partitions, which operating system each partition uses, and which partition the computer will boot from.

**pathname** — The location of a file or folder on a disk. For example, if a file named QTR1.DOC is stored in the folder OFFICE on drive C:, the pathname for the file is C:\OFFICE\QTR1.DOC

**polymorphic virus** — A type of virus that changes its telltale code segments so that it "looks" different from one infected file to another, thus making detection more difficult.

**program** — An executable file or group of files written for a specific purpose such as word processing or creating a spreadsheet.

**program virus** — A virus that infects executable program files, such as .COM, .EXE, .OVL, .DRV (driver), and .SYS (device driver) files.

**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.

**registry** — A database maintained by Windows NT to store hardware and software configuration information.

**repair** To remove a virus from a file or boot record and return the item to its original, uninfected state.

**scan** The systematic search for viruses that is performed by Norton AntiVirus.

**stealth virus** A virus that actively seeks to conceal itself from discovery or defends itself against attempts to analyze or remove it.

**subdirectory** *See* subfolder.

**subfolder** A folder within a folder.

**system files** The files that make up the operating system.

**trojan horse** A program that promises to be something useful or interesting (like a game), but covertly may damage or erase files on your computer while you are running it. Trojan horses are not viruses because they don't replicate and spread.

**virus** A self-replicating program written intentionally to alter the way your computer operates without your permission or knowledge.

**virus definition** Virus information that allows Norton AntiVirus to recognize and alert you to the presence of a specific virus.

**write-protected disk** A disk that cannot be written to. Write-protecting disks prevents viruses from infecting them. To write-protect a 5.25" disk, cover the notch on the side of the disk with an adhesive label (usually a tab included with boxes of disks). To write-protect a 3.5" disk, slide the lever on the back of the disk to uncover the hole through the disk.

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

# Symantec Service and Support Solutions

Symantec is committed to excellent service worldwide. Our goal is to provide you with professional assistance in the use of our software, wherever you are located.

Technical Support and Customer Service solutions vary by country. If you are outside the United States or Canada, please refer to the Worldwide Service and Support section at the end of this chapter.

## Registering Your Symantec Product

You can register via your modem during the installation process if your Symantec software offers this feature. In addition, you can use the toll-free fax number listed below to register your product.

If your address changes, you can mail or fax your new address to Customer Service. Please send it to the attention of the Registration Department.

Symantec Corporation
Attn: Registration Dept.
175 W. Broadway
Eugene, OR 97401

(800) 800-1438 Fax

## Technical Support

Symantec's Technical Support department offers expanded support options designed for your individual needs and to help you get the most out of your software investment.

The phone numbers listed on the back of this manual are for support in North America. If you are outside the United States or Canada, please call the local Symantec office or distributor in your area, or refer to the information provided at the end of this chapter.

Symantec now offers different types of technical support services for you to choose from, which are described below.

## Virus Hotline

The Norton AntiVirus group of Symantec Corporation, as part of its continuing commitment to halt the spread of computer viruses, has set up a special telephone hotline to help you recover from any virus emergency—regardless of which antivirus software you may use. To get help, or just answers to virus questions, call the following telephone number:

(541) 9VIRUS9

(541) 984-7879

Technicians are available to take your calls from 7:00 a.m. until 4:00 p.m. (Pacific Daylight Time), Monday through Friday, excluding holidays.

## PriorityCare Support

All registered users of Symantec products are entitled to these services on a "pay-as-you-go" basis:

- The PriorityCare 800-number is charged to your VISA, MasterCard, or American Express on a per incident basis.
- The PriorityCare 900-number is charged to your telephone bill on a per minute basis. (As of this writing, the equivalent 900-number service is not available outside the United States.)
- Average hold time will be kept to a minimum.
- PriorityCare Support is available Monday through Friday, 6:00 a.m. to 5:00 p.m. Pacific Time.

To use the PriorityCare 800- and 900-number services, please refer to those numbers on the back of this manual.

## PremiumCare Support

All registered users of Symantec products are entitled to these services on an annual subscription basis:

### PremiumCare Gold Support

- Unlimited calls on a toll-free 800 line.
- Average hold time will be kept to a minimum.
- PremiumCare Gold Support is charged on an annual subscription basis.
- PremiumCare Gold Support is available Monday through Friday, 6:00 a.m. to 5:00 p.m. Pacific Time.

### PremiumCare Platinum Support

- Unlimited calls on a toll-free 800 line.
- Average hold time will be kept to a minimum.
- A Support Center Manual with troubleshooting, installation, configuration, and usage information.
- Quarterly updates of technical notes and bulletins.
- Instant access to senior support staff.
- Automatic updates of inline software revisions. (Inline software revisions do not include version upgrades.)
- After hours and weekend support is also available to PremiumCare Platinum customers for an additional fee.
- PremiumCare Platinum Support is charged on an annual subscription basis per product family. The annual fee is for two subscribers; other subscribers can be added on a per person basis.
- PremiumCare Platinum Support is available Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

To order PremiumCare Gold or Platinum support, please contact Customer Service or your Symantec sales representative.

## Electronic Support

Technical information is available 24 hours a day on electronic bulletin board systems. Symantec provides access to its own Symantec bulletin board system (BBS), and maintains the Symantec forums on CompuServe and America Online.

## Symantec BBS

The Symantec BBS provides a Customer Service forum, shareware and public-domain software, “Frequently Asked Questions” (FAQs), and support forums where you can exchange tips and information with other users. Settings for the Symantec bulletin board are: 8 data bits, 1 stop bit; no parity, and baud rates from 300 to 28.8K are available.

| | |
|---|---|
| 300- through 14,400-baud modems | (541) 984-5366 (24 hrs.) |
| 300- through 28,800-baud modems | (541) 484-6669 (24 hrs.) |

## CompuServe

You can exchange information and ideas with Symantec representatives and with other users of Symantec products on the CompuServe bulletin board.

To access the Symantec forums on CompuServe, type:

`GO SYMANTEC` at any ! prompt.

For additional information, or to subscribe in the United States and Canada, please call CompuServe at (800) 848-8199. Outside the United States and Canada, please call (1) (614) 529-1340. Check with CompuServe for data communications settings.

## America Online

To access the Symantec bulletin board on America Online, type keyword:

`SYMANTEC`

For additional information, or to subscribe in the United States and Canada, please call America Online at (800) 227-6364. Check with America Online for data communications settings.

## Automated Fax Retrieval System

Symantec’s automated fax retrieval system can be used 24 hours a day to receive product information on your fax machine. You can call from any touch tone phone to receive an index listing of both Technical Support and Customer Service documents available, then have any of these specific documents faxed to you.

To receive technical application notes and samples of "how tos," please call our Technical Support fax retrieval number, and choose Option 2.

You can receive general product information, data sheets, and product upgrade order forms from our Customer Service fax retrieval number.

- Technical Support: (541) 984-2490
- Customer Service: (800) 554-4403

In addition, you can receive a listing of Symantec offices and worldwide service and support partners by calling the Technical Support fax retrieval number, choosing Option 2, and requesting Document 1400.

## Customer Service

Symantec's Customer Service department builds and maintains long-lasting customer relations through consistent, expert service. Our Customer Service department is available to help you:

- Order an upgrade.
- Subscribe to the technical support solution of your choice.
- Fulfill your request for product literature or demonstration disks.
- Find out about dealers and consultants in your area.
- Replace missing or defective pieces (disks, manuals, etc.) from your package.
- Update your product registration with address or name changes.

For specific questions about how to use your Symantec software, please contact Technical Support.

## Service and Support Headquarters

Symantec's service and support headquarters for North America is at the following location.

| | | |
|---|---|---|
| **USA** | Symantec Corporation<br>175 W. Broadway<br>Eugene, OR 97401 | (800) 441-7234 (USA & Canada)<br>(541) 334-6054 (all other locations)<br>Fax (541) 334-7400 |

# Worldwide Service and Support

Symantec provides technical support and customer service worldwide. Services vary by country and include International Partners (IPs) who represent Symantec in regions where there is no Symantec office. Most IPs provide customer service and technical support for Symantec products in your local language, as close to your home or office as possible.

If your country is not listed in the International Locations section below, please call our Technical Support automated fax retrieval service, located in the United States, at (541) 984-2490, choose Option 2, and request Document 1400.

## International Locations

**European Headquarters**

| | |
|---|---|
| Symantec Europe Ltd.<br>Kanaalpark 145<br>2321 JV Leiden<br>The Netherlands | Tel. (31) (71) 535 3111<br>Fax (31) (71) 535 3150 |
| Customer Service | Tel. (31) (71) 535 3294 |
| Technical Support | |
| Dutch | Tel. (31) (71) 579 4407 |
| French PC/Mac | Tel. (33) (1) 41 38 69 80 |
| French Mac | Tel. (33) (1) 41 38 69 81 |
| German | Tel. (49) (211) 9917 110 |
| English | Tel. (44) (1628) 788 580 |
| Other Countries | Tel. (31) (71) 579 4425<br>Fax (31) (71) 535 3153 |
| BBS | Tel. (31) (71) 535 3169 |
| BBS | Tel. (31) (71) 532 2852 |
| BBS SAM Virus Definition Update | Tel. (31) (71) 535 3299 |
| Automated fax retrieval | Tel. (31) (71) 535 3255 |

**Asia/Pacific Rim region**

| | |
|---|---|
| Symantec Australia Pty. Ltd.<br>408 Victoria Road<br>Gladesville, NSW 2111<br>Australia | Tel. (61) (2) 879 6577<br>Fax (61) (2) 879 6805 |
| Technical Support | Tel. (61) (2) 879 6577<br>Fax (61) (2) 879 6594 |
| BBS | Tel. (61) (2) 879 6322 |
| DOS/Win Antivirus recording | Tel. (61) (2) 879 7362 |
| Mac Antivirus recording | Tel. (61) (2) 879 6968 |

**Brazil**

| | |
|---|---|
| Symantec Brazil<br>AV. Irai, 79 - 1 o. andar - conj 11A<br>Sao Paulo - SP 04082-020 | Tel. (55) (11) 289 9420<br>Fax (55) (11) 287 9824 |

**México**

| | |
|---|---|
| Symantec México<br>Rubén Dario No. 36, Piso 2, OFNA 6<br>Colonia Chapultapec Polanco<br>Col. Rincón del Bosque<br>11560 México, D.F. | Tel. (52) (5) 545 1234<br>Fax (52) (5) 531 2252 |
| Technical Support | For Technical Support call the automated fax retrieval service, located in the United States, at (541) 984-2490, and request Document 1400. |

Every effort has been made to ensure the accuracy of this document. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change, without prior notice.

THIS PAGE LEFT BLANK INTENTIONALLY

# Index


## A

access privileges, 75
Activity Log
    customizing, 65–66
    filtering entries in, 40
    finding files requiring replacement, 46
    unable to update, 71
    viewing all entries in, 39
Activity Log Filter dialog box, 40
adding
    exclusions to exclusions list, 64–65
alert boxes
    appearance on screen, 34
    command buttons, 44–45
    responding to, 43
alerts
    customizing, 67–68
    customizing response method, 58
    described, 19
    generating immediately, 34, 43
    responding to
        methods of removing viruses, 45–47
        virus alert, 45
    situations triggering, 43
Alerts tab, 67
America Online, virus definition updates via, 51
audible alarms, enabling, 67
automatic scans, 38

## B

backup files
    creating before repairing, 62
    deleting virus-infected, 62
BBSs (bulletin board systems)
    defined, 75
    scanning downloaded files from, 32
boot record program
    *See also* boot records; boot viruses
boot records
    bypassing scans of, 37
    defined, 75
    repairing infected, 46
        automatically, 59
        unsuccessfully, 47
    scanning, 38, 58
    system messages
        unable to repair write-protected, 71
    unsuccessful repairs to, 47
boot viruses
    defined, 75
    described, 20
    removing, 46
    scanning for, 58
    viewing lists of, 55
booting computers
    defined, 75
    when a virus is found, 73
bulletin board systems (BBSs)
    defined, 75
    scanning downloaded files from, 32
    virus definition updates via, 51

## C

closing Activity Log, 39
cold boots, 75
command buttons, alert box, 44–45
command-line switches, 41
    defined, 75
common viruses, viewing lists of, 55
compressed files
    defined, 75
    message warning of virus in, 69

removing viruses from, 47
scanning, 58
CompuServe, virus definition updates via, 51
context-sensitive help, accessing, 27–29
customizing
Activity Log, 65–66
alerts, 67–68
general scan options, 57–63
manual scan options, 60
response to alerts, 58
scanner options, 57–62

## D

data files, 76
deleting
exclusions, 65
infected files
automatically, 59
in response to alerts, 45, 46
irreparably damaged files, 47
program file extensions, 62
virus definitions, 55
virus-infected backup files, 62
detection methods, virus, 18
disabling
boot record scans, 37
scheduled scans, 38
drives
error message for, 69
preselecting for scans, 60
scanning, 14, 32
system messages
unable to access, 70
unable to repair boot record, 71
virus found, 69
droppers, 76

## E

editing
exclusions, 65
enabling
audible alarms, 67
scheduled scans, 38
excluding files from scans, 60
exclusions
defined, 76
described, 63
removing and modifying, 65
exclusions list
adding entries to, 64–65
unable to update, 71
viewing, 64
Exclusions tab, 64
exclusions. *See also* exclusions list
executable file, 76
exiting Norton AntiVirus, 31

## F

files
adding to exclusions list, 64–65
deleting infected, 45, 46, 59
re-infected by removed viruses, 48
repairing infected, 46
requiring replacement, finding, 46
scanning individual, 14, 33
selecting for scanning, 36–37
system messages, 69
unable to delete write-protected, 70
unable to repair, 71
virus found, 70
types infected by viruses, 17, 36
unsuccessful repairs to, 47–48
filtering Activity Log entries, 40
floppy disks
repairing infected, 46
unsuccessful repairs to, 48
virus definition updates via, 53
folders, 33
defined, 76
excluding from scans, 65
scanning for viruses, 14, 33

## G

general scanning options, 62–63

General Settings tab, 63

## H

How To... HELP menu command, 28

## I

infected files and boot records
    defined, 76
    deleting, 45, 59
    repairing, 46
infections. *See* virus attacks
installing
    Norton AntiVirus, 13
        post-installation recommendations, 26–27
    virus definition files, new, 53
Internet, virus definition updates via, 52

## K

known viruses
    excluding files from scans, 63
    viewing a list of, 54
    viewing report of detections, 39

## L

.LHA files, 76

## M

macro virus
    defined, 76
    scans for, 61
main window, 32
master boot record
    defined, 76
    scanning, 38, 58
    system messages
        virus found, 70
messages, system, 69–71
multipartite viruses
    defined, 77
    viewing lists of, 55

## N

NAVOPTS.DAT file not found message, 69
network drives
    scanning, 60
New Exclusion dialog box, 65
Norton AntiVirus
    exiting, 31
    installing, 13, 25–26
    main window, 32
    starting, 14, 31
    uninstalling, 27
    virus protection technologies, 19
Norton AntiVirus main window, 14, 32

## O

online help, 29
opening context-sensitive help, 27–29
operating system, 77

## P

partition table defined, 77
pathnames, 77
polymorphic viruses
    defined, 77
    viewing lists of, 55
preventing virus attacks, 18
printing
    Activity Log, 39
    inability to, 70
    scan results, 35
    virus list, 55
Problems Found dialog box
    described, 34
    responding to, 44
    situations causing display of, 19, 43
program file extensions
    adding to list, 61
    removing from list, 62
    resetting list of, 62

specifying for scans, 37, 58, 61–62
viewing current, 61
Program File Extensions dialog box, 61
program files
enabling scans of, 37, 58
failure to execute after repair, 49
repairing infected, 46
program viruses
defined, 77
described, 20
viewing lists of, 55

## R

read-only disks and files, 77
rebooting computer, 77
recovering from virus emergencies, 18
removing
program file extensions, 62
viruses
from compressed files, 47
from files and boot records, 45–47
repairing files and boot records, 46
automatically, 59
defined, 78
failure to execute properly after, 49
in response to alerts, 46
reports, viewing activity log, 39

## S

Scan dialog box, 33
SCAN menu
FILE... command, 33
FOLDERS... command, 33
Scan Results dialog box, 35
scan results, viewing and printing, 35
Scanner Advanced Settings dialog box, 60
Scanner Settings dialog box, 57
scanning manually, 32
scans
customizing, 57–60
general scanning options, 57–63
specifying program file extensions, 61–62
defined, 78
initiating, 32–35
scheduling, 38–39
stopping scans, 60
unable to complete, 70
viewing date/time occurred, 40
Scheduler Service, 42
Scheduler. *See* scheduling virus scans
scheduling virus scans, 38
searching for virus names, 55
starting Norton AntiVirus, 14, 31
stealth viruses
defined, 78
viewing lists of, 55
subfolders
defined, 78
excluding from scans, 65
Symantec BBS, virus definitions from, 52–53
system files
defined, 78
unsuccessful repairs to, 47
system messages, 69–71

## T

trojan horses, 78

## U

uninstalling Norton AntiVirus, 27
updates, virus definition, 19, 51

## V

viewing
Activity Log, 39, 65–66
exclusions list, 64
virus list, 54–55
VIR file extension
specifying alternative to, 62
described, 46
deleting files with, 46
virus attacks

about, 18
virus definitions
*See also* virus definitions file
defined, 78
deleting, 55
updates, 51–54
virus definitions file
*See also* virus definitions; virus list
reasons for updating, 19
unable to find, 70
updating, 51–53
virus life cycle, 18
virus list
*See also* virus definitions
changes to, 40
viewing and printing, 54–55
Virus List dialog box, 54
virus signatures, 19
viruses
avoiding, 31
damage caused by, types of, 17
defined, 17, 78
files re-infected by removed, 48
life cycle, 18
message warning of detection of, 69
removing, 46
scanning for, 32
sources of, 18
spread mechanisms, 18
viewing names and descriptions of, 54–55

## W

what to do after installation, 26
write-protected disks, 78

## Z

ZIP files, 78
removing viruses from, 47
scanning for viruses, 58