

Norton AntiVirus for Windows 95/98

User's Guide

NORTON

AntiVirus[™]

VERSION 5.0

Norton AntiVirus for Windows 95/98 User's Guide

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

Copyright Notice

Copyright © 1990-1998 Symantec Corporation.

All Rights Reserved.

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

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

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

Trademarks

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

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

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THE LICENSE AGREEMENT.

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

LICENSE AND WARRANTY

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

You may:

- (i) use that number of copies of the appropriate titles of the software as have otherwise been licensed to you by Symantec under a Symantec Volume Incentive or Value License, provided that the number of copies of all such titles in the aggregate will not exceed the total number of copies so indicated on such Volume Incentive or Value license;
- (ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
- (iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
- (iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
- (v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

You may not:

- (i) copy the printed documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software;
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- (iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed;
- (v) use the server based software products included with the Software if you have not licensed the Norton AntiVirus Solution for server-based products;
- (vi) use the suite based software products included with the Software if you have not licensed the Norton AntiVirus Solution Suite;
- (vii) use other than the Macintosh versions of the software if you have only licensed the Macintosh versions of the software; or
- (viii) use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version.

Limited Warranty:

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

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

Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

U.S. Government Restricted Rights:

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

General:

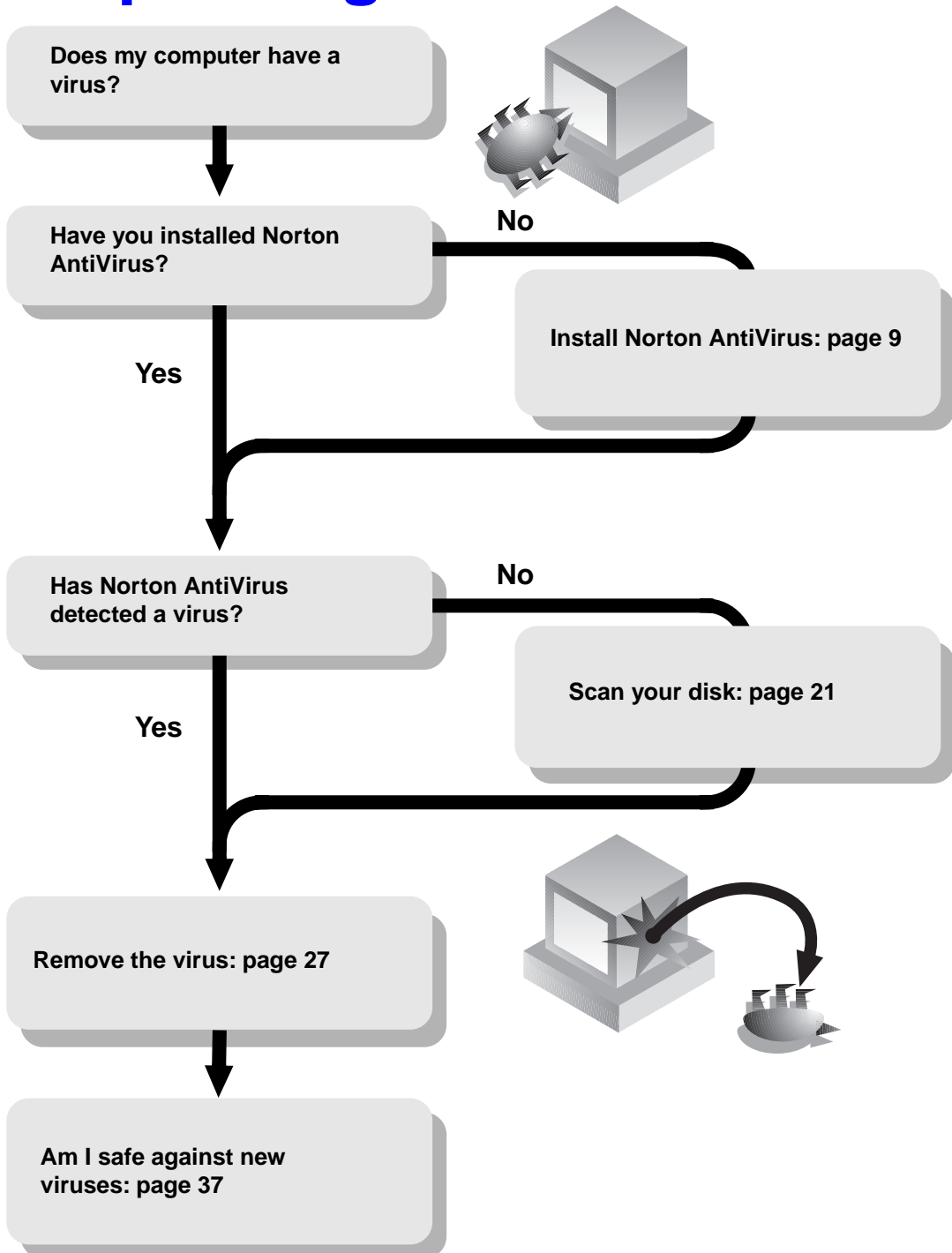
This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you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

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

SYMANTEC SOFTWARE LICENSE ADDENDUM

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

Help! I've got a virus!



C O N T E N T S

Chapter 1 Installation

Norton AntiVirus for Windows 95/98	9
Requirements for installing	9
Installing Norton AntiVirus for Windows 95/98	10
Questions when installing	10
Testing the Norton Rescue Boot Disk	12
If you didn't create Rescue Disks	12
Uninstalling Norton AntiVirus for Windows 95/98	13

Chapter 2 Using Norton AntiVirus for Windows 95/98

What Norton AntiVirus does automatically	16
What you have to do	16
Tips for avoiding viruses	17
Turning Norton AntiVirus Auto-Protect off temporarily	18
If you didn't create Rescue Disks	19
What else can I do with Norton AntiVirus?	20
Start Norton AntiVirus	20
Get help	21
Scan for viruses	21
Schedule virus scans	22
Update your Norton AntiVirus Rescue Disks	23
Customize Norton AntiVirus	24
Quarantine infected or suspicious files	24
Submit a potentially infected file to SARC for analysis	25
What to do if a virus is found	27
Quick guide to alert actions	28
Types of virus alerts	29
VIRUS FOUND	29
VIRUS IN MEMORY	29
INOCULATION CHANGE	30
VIRUS-LIKE ACTIVITY	30
What to do if Norton AntiVirus can't repair	32
Infected files	32
Compressed files	33
Hard disk master boot record or boot record	34
Floppy disk boot record	34
System file	34
Using Rescue Disks in virus emergencies	35
Restoring your hard disk	36
What to do first	36

Keeping virus protection current	37
How to update virus protection	37
Updating virus protection with LiveUpdate	37
Using LiveUpdate Email	38
Scheduling automatic LiveUpdates	38
Updating virus protection without LiveUpdate	39
Updating your Norton AntiVirus rescue disks	40
Troubleshooting	41
Command-line switches	44

Potential Virus Submission Procedure

Index

Installation

Norton AntiVirus for Windows 95/98

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

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

Requirements for installing

Your minimum computer requirements are:

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

You also must have:

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


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

Installing Norton AntiVirus for Windows 95/98

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

To install Norton AntiVirus for Windows 95/98:

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

If the Norton AntiVirus setup program does not start automatically, Autorun may be disabled on your computer.
 -  ■ To manually start Norton AntiVirus setup from a CD, insert the Norton AntiVirus CD in your CD-ROM drive, double-click the My Computer icon on the Windows desktop, double-click your CD-ROM drive, then locate and double-click Setup.
 - To install from floppy disks, insert Norton AntiVirus Disk 1 in the A: drive, click Start on the Windows taskbar, click Run, type `A:SETUP` in the text box, then click OK.
- 2 Follow the on-screen instructions. Questions? See [page 10](#).
- 3 Test the Norton Rescue Boot Disk that you created during installation. See [page 12](#) for testing details.

Questions when installing

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

Table 1-1

What the choices are	What you should do	Why
Select the folder for Norton AntiVirus.	Accept the preset choice: C:\Program Files\Norton AntiVirus	There's no reason not to. The choice is there for unusual circumstances.
Schedule weekly scans of your local hard disks that run automatically.	Leave this checked.	A weekly scan makes sure your disks stay virus-free.
Enable Auto-Protect.	Leave this checked.	Auto-Protect constantly monitors your computer to make sure a virus does not gain entry.
Scan at startup.	Leave this checked.	Makes sure critical system files are virus-free every time you start up.
Run LiveUpdate after installation.	Leave this checked if you have a modem or an Internet connection.	LiveUpdate connects to a special Symantec site and updates Norton AntiVirus automatically to protect you against newly discovered viruses.
Do you wish to create Rescue Disks?	We strongly recommend that you create the Rescue Disks.	Rescue Disks can save you from disaster if your computer becomes infected with certain types of viruses.
Scan for viruses after installation.	Leave this checked.	Makes sure that your computer is virus-free.
Norton AntiVirus has detected a Netscape browser. Do you want to install plug-ins?	Choose Yes.	This option allows Norton AntiVirus to scan files for viruses when you download using a Netscape browser.
Would you like to restart your computer?	Select Yes, I want to restart my computer now.	When your computer restarts, you are fully protected against viruses.

Testing the Norton Rescue Boot Disk

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

To test your Norton Rescue Boot Disk:

- 1 Click Start on the Windows taskbar, click Shut Down, select Shut Down Your Computer, and click OK.
- 2 Turn off the power.
- 3 Insert the first disk of your Norton AntiVirus rescue disk set, labelled "Norton Rescue Boot Disk," in the A: drive, then restart your computer.
- 4 After your computer starts, type `TEST` at the `A:\` prompt and press Enter.

A screen message reports whether your Norton Rescue Boot Disk works properly.

Note: Your Norton Rescue Boot Disk doesn't work? See [page 41](#).

- 5 Remove the disk from the A: drive and slide open the plastic tab on the back of the disk to write-protect it. This prevents you from accidentally changing the data stored on the disks.
- 6 Turn the power off and on again to restart your computer.
Because you didn't start Windows for this test, you don't have to perform your usual Windows Shutdown first.

If you didn't create Rescue Disks

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

To create Rescue Disks:

- 1 On the Windows taskbar, click Start, point to Programs, point to the Norton AntiVirus group, then click Rescue Disk.
- 2 Follow the on-screen instructions.
- 3 Test your Norton Rescue Boot Disk.

See "[Testing the Norton Rescue Boot Disk](#)" on page 12.

Uninstalling Norton AntiVirus for Windows 95/98

To uninstall Norton AntiVirus:

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

Using Norton AntiVirus for Windows 95/98

A computer virus is, simply, a computer program written by an ill-intentioned programmer. Your computer can catch a virus from disks, a local network or the Internet. Just as a cold virus attaches itself to a human host, a computer virus attaches itself to a program. And just like a cold, it's contagious.

What viruses do

- Take control of your computer without your knowledge.
- Cause your computer to behave strangely, for example, beep or display annoying messages.
- Hide in macros that infect and spread throughout Word and Excel documents. (These are called macro viruses.)
- Cause serious destruction to your files. Viruses can damage data, delete files, and can even completely erase your hard disk.
- Remain inactive until a predetermined trigger date (for example, Friday the 13th) to wreak havoc.

What viruses don't do

- Infect or damage hardware, such as keyboards or monitors. You may experience strange behaviors (such as characters appearing upside down) but your disks are not physically damaged, just what's stored on them.

What Norton AntiVirus does automatically

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

- Eliminates viruses and repairs files.
- Makes sure your computer is safe from viruses at startup.
- Checks for viruses every time you use software programs on your computer, floppy disks, and document files that you receive or create.
- Monitors your computer for any unusual activities that may indicate an active virus.
- Runs a scheduled scan automatically once per week to confirm that your hard disks are virus-free.
- Protects you from Internet-borne viruses. No separate programs or options changes are necessary. Auto-Protect scans program and document files automatically as they are downloaded and files within compressed files when they are extracted.

What you have to do

To update virus protection, see page 37.

To update rescue disks, see page 23.

- Regularly obtain from Symantec updated information that Norton AntiVirus needs to keep your virus protection up-to-date. You can do this online (for example, over the Internet).
- Update your Norton AntiVirus Rescue Disks each time you get the latest virus protection files or make changes to your computer's hardware or operating system (for example, when you add a disk drive).

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

Tips for avoiding viruses

To avoid computer viruses, follow these rules:

- Get in the habit of looking for the Norton AntiVirus Auto-Protect icon in the taskbar on your Windows desktop. Be sure Norton AntiVirus Auto-Protect is turned on (enabled) at all times.
- Regularly get the latest virus protection files from Symantec to keep up with the new viruses that have been released since you purchased Norton AntiVirus.
- Buy legal copies of all software you use and make write-protected backup copies.
- Scan all files on disks you receive from other people.

*To scan disks, see
page 21.*

Turning Norton AntiVirus Auto-Protect off temporarily

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

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



To turn off Norton AntiVirus Auto-Protect temporarily:

Do one of the following:

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



To turn on Norton AntiVirus Auto-Protect:

Do one of the following:

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

If you didn't create Rescue Disks

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

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

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

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

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

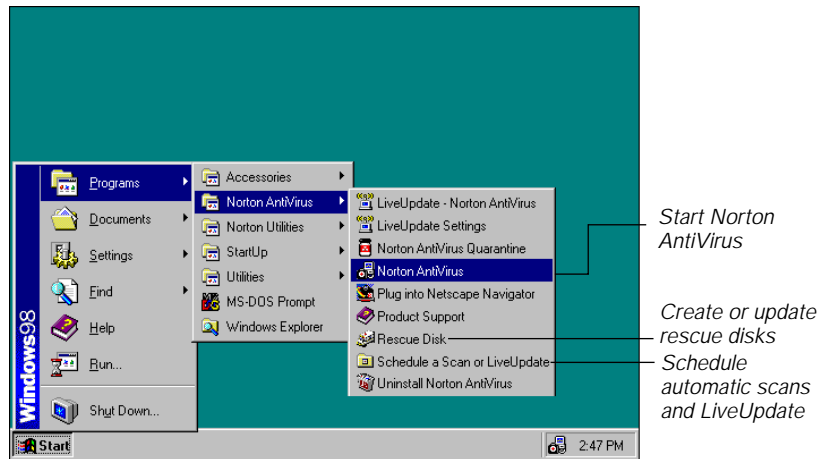
To create Rescue Disks:

- 1 On the Windows taskbar, click Start, point to Programs, point to the Norton AntiVirus group, then click Rescue Disk.
- 2 Follow the on-screen instructions.
- 3 Test the first disk in your Rescue Disk set called "Norton Rescue Boot Disk" to make sure it will start your computer in an emergency situation.

See "[Testing the Norton Rescue Boot Disk](#)" on page 12.

What else can I do with Norton AntiVirus?

From the Norton AntiVirus group on the Start menu (which Windows created when you installed Norton AntiVirus), you can access several Norton AntiVirus features.

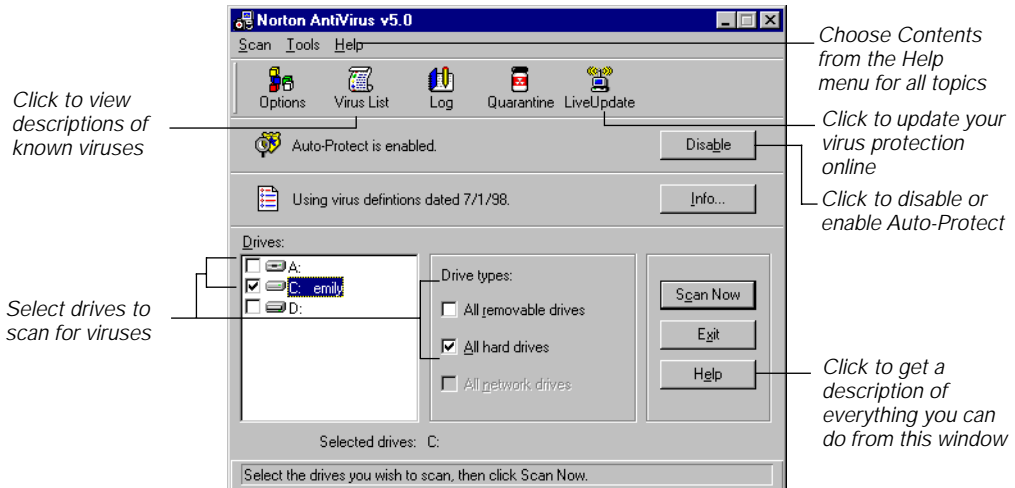


Start Norton AntiVirus

WHY? From the Norton AntiVirus main window you can initiate scans, change how Norton AntiVirus works, or click LiveUpdate to get the latest virus protection files directly from Symantec.

To open the Norton AntiVirus window:

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



Get help

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

To get help using Norton AntiVirus:

Do one of the following:

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

Scan for viruses

WHY? We recommend you scan all floppy disks before you use them.

To scan drives for viruses:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window, do one of the following:
 - Check specific drives in the Drives list box.
 - Select multiple drives by checking items in the Drive types box.
- 3 Click Scan Now.

To scan individual files or folders for viruses:

- 1 Start Norton AntiVirus.
- 2 From the Scan menu at the top of the Norton AntiVirus main window, choose Folders, Path, or File.
- 3 Make your choice and click Scan.

Tip: To quickly scan a drive, folder, or file, right-click an item in a My Computer or Windows Explorer window and choose Scan With Norton AntiVirus in the menu that pops up.

Schedule virus scans

WHY? A weekly scheduled scan is an additional reassurance that your computer is virus-free. If you accepted the preset options when you installed Norton AntiVirus, a scan is already scheduled to run once per week automatically.

Note: Norton AntiVirus for Windows 98 and Windows 95 use different schedulers. The Windows 98 version uses the new built-in Windows scheduler, while the Windows 95 version uses the Norton Program Scheduler.

To schedule a scan for Windows 98:

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

To schedule a scan for Windows 95:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window, click Scheduler.
- 3 Click Add.
- 4 Select Scan For Viruses for the Type Of Event.

- 5 The /L in the What To Scan text box tells Norton AntiVirus to scan all local drives. You can also enter specific drive letters (for example, C: D:) instead.
- 6 Select Weekly for the Frequency.
- 7 Click OK to close the dialog box, then click OK again to confirm.
- 8 Click the Exit button in the upper-right corner of the Norton Scheduler dialog box, then click Minimize to close the dialog box but leave the Norton Scheduler running.

Your computer must be turned on and Norton Scheduler must be running when the scan is due to take place.

Update your Norton AntiVirus Rescue Disks

To update virus protection, see [page 37](#).

WHY? The information stored on your Rescue Disks needs to change whenever you install new hardware, add or change an operating system, repartition your hard disk, or update your virus protection. Using outdated Rescue Disks could cause serious problems.

When you update your Norton AntiVirus Rescue Disks, you create a new set of disks.

To update your Norton AntiVirus rescue disk set:

- 1 On the Windows taskbar, click Start, point to Programs, point to the Norton AntiVirus group, and click Rescue Disk.
- 2 If you are re-using your current Rescue Disks, make sure they are not write-protected. Slide the small plastic tab on the back side of each disk closed.
- 3 Follow the on-screen instructions.
- 4 Click OK when prompted to format the disks.

This step replaces the old information with new information.

- 5 When updated, write-protect the disks by sliding open the plastic tab on the back side of each disk.

This prevents you from accidentally changing the data stored on the disks.

- 6 Test the Norton Rescue Boot Disk. See [page 12](#) for testing details.

Customize Norton AntiVirus

WHY? Norton AntiVirus is preset to provide you with complete protection against viruses. It is unlikely you need to change any settings. However, Norton AntiVirus provides options for users (for example, system administrators) who want to customize the way virus protection works.



To customize Norton AntiVirus protection:

- 1 Start Norton AntiVirus.
- 2 Click the Options button in the Norton AntiVirus main window.
- 3 Click one of the tabs in the Options dialog (for example, Alerts).
The dialog changes to show options for the selected feature.
- 4 Click Help to get information about options.
- 5 Make your changes and click OK to exit.

Tip: Right-click an option and choose What's This for an explanation of the option.

Quarantine infected or suspicious files

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

Files are placed in the Quarantine in one of three ways:

- You selected Quarantine after receiving a Norton AntiVirus alert.
- You open the Quarantine and click Add Item to manually select a file and add it to the Quarantine.
- Norton AntiVirus is configured to quarantine infected items rather than repair them or to quarantine them if they cannot be repaired.



To re-scan a file isolated in the Quarantine:

- 1 Start Norton AntiVirus.
- 2 Click the Quarantine button in the Norton AntiVirus main window.
- 3 Click LiveUpdate in the Quarantine window.

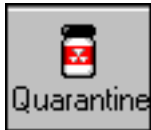
Your installed set of virus definitions files is updated with the latest definitions automatically.

- 4 Select the file in the Quarantine and click Repair Item.
The file is scanned again with the new definitions.

Submit a potentially infected file to SARC for analysis

WHY? The Symantec AntiVirus Research Center (SARC) will analyze your file to make sure it is not infected. If a new virus is discovered in your submission, SARC will create and send you special updated virus definitions to detect and eliminate the new virus.

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



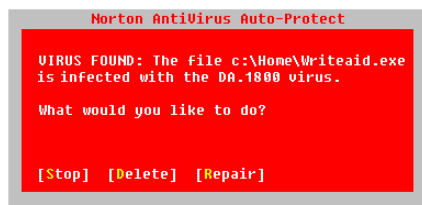
To submit a file to SARC:

- 1 Start Norton AntiVirus.
- 2 Click the Quarantine button in the Norton AntiVirus main window.
- 3 Select a file in the list of Quarantined items and click Submit Item.

Follow the directions in the Wizard to collect the necessary information and submit the file for analysis.

You are notified by email with the results of the analysis.

What to do if a virus is found

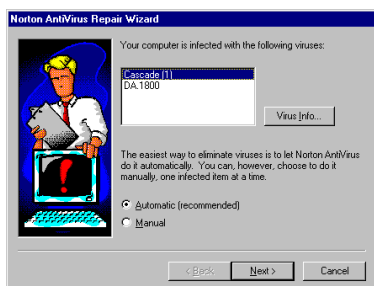


If you see a virus alert

- 1 Look for words that identify the type of problem. Read the whole message.
- 2 Press Enter to choose the action that is preselected for you, or type the first letter of the action you want to take (for example, type R for Repair).

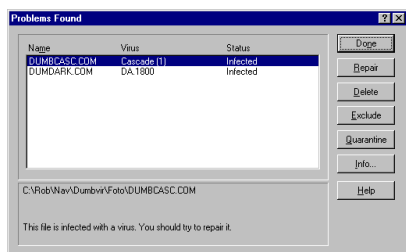
If you need more information, do one of the following:

- See [“Quick guide to alert actions”](#) on page 28. for more information.
- Find the type of problem in the next few pages. For example, if the message says VIRUS FOUND, look for “VIRUS FOUND.”



If you see the Norton AntiVirus Repair Wizard

- Click Next to have Norton AntiVirus automatically get rid of the virus.



If you see the Problems Found dialog








- 1 Highlight an entry in the list box.
- 2 Read the message at the bottom of the dialog box.
- 3 Click Repair when infected files are found.

See [“Quick guide to alert actions”](#) on page 28. for information about the other actions.

Quick guide to alert actions

If a Norton AntiVirus alert appears on your screen, use this table to decide what to do. If you need more information, see the next section, “Types of virus alerts,” for step-by-step instructions.

Note: In some situations, your mouse won’t work when an alert appears. In these cases, type the first letter of your selection (for example, type R for Repair) or just press Enter to accept the recommended selection.

Actions	When and why you use them
	For a VIRUS FOUND, Repair is always the best choice. Repair eliminates the virus and repairs the infected item automatically.
	Erases both the virus and the infected file. The virus and file are gone forever. Replace a deleted file from the original program disks or backup copy. If the virus is detected again, your backup copy or original disk is infected.
	Stops the current operation to prevent you from using an infected file. Stop does not solve the problem. You’ll be alerted again the next time you do the same thing.
	Continues the current operation. Choose Continue only if you are sure a virus is not at work. You’ll be alerted again. If you’re not sure what to do, choose Stop.
	If you choose Exclude and a virus is at work, the virus won’t be detected. Exclude should be used only by system administrators for system tuning.
	<p>For an INOCULATION CHANGE, Inoculate updates the stored inoculation data for a boot record that has changed since it was last inoculated. Inoculation changes fall into two categories:</p> <ul style="list-style-type: none">▪ Expected: If you’ve just finished a system upgrade, the boot records may change. In this case, choose Inoculate. For example, if you’ve just upgraded your computer to Windows 98 from Windows 95, choose Inoculate. This is an expected change.▪ Unexpected: Changes to boot records are usually caused by viruses. If you have not recently performed an upgrade, choose Repair. <p>Caution: Choosing the wrong option for an inoculation change can corrupt your disk.</p>
	Isolates the virus-infected file, but does not remove the virus. Choose Quarantine if you suspect the infection is caused by an unknown virus and you want to submit the virus to the Symantec AntiVirus Research Center for analysis.

Types of virus alerts

VIRUS FOUND

When Norton AntiVirus finds a virus has infected a file on your computer, it produces a warning something like this:

VIRUS FOUND: The BADVIRUS virus was found in C:\MYFILE.

To get rid of a virus infection:

- Type R for Repair.

Your file is restored to exactly the way it was before the virus infected it. That's all you need to do. If the repair was successful, the virus is gone and your computer is safe.

Norton AntiVirus can't repair? See [page 32](#).

VIRUS IN MEMORY

Norton AntiVirus stops your computer when it finds a virus in memory. While you don't normally turn off a computer without first exiting Windows, in this case it is necessary because your computer is halted. You can't do anything else.

WHY? A virus in memory is active, dangerous, and will quickly spread to many other files.

A memory virus warning says something like this:

VIRUS IN MEMORY. The BADVIRUS virus was found in memory.

Computer is halted. Reboot from your write-protected rescue disk, then scan your drive again.

To get rid of a virus in memory:

- 1 Turn off your computer using the power switch.
- 2 Insert your Norton AntiVirus Rescue Disk labeled "Norton Rescue Boot Disk" into the A: drive.

- 3 Turn the computer on using the power switch.
Don't have a Norton Rescue Boot Disk? See [page 19](#).
- 4 Follow the on-screen directions.
Can't boot from the A: drive? See [page 41](#).

INOCULATION CHANGE

If Norton AntiVirus detects any changes made to the stored information it keeps about inoculated boot records, it alerts you. For example, the alert may say something like this:

INOCULATION CHANGE: The boot record on drive C:\ has changed since it was last inoculated.

To respond to an inoculation change alert, do one of the following:

- Type I for Inoculate if the change is expected.
If you've just upgraded your computer to Windows 98 from Windows 95, choose Inoculate. This change is expected.
- Type R for Repair if the change is not expected.
For example, if you know no one has recently made changes to your system like the one described above, you should choose repair.

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

VIRUS-LIKE ACTIVITY

A virus-like activity alert does not necessarily mean that your computer has a virus. It's simply a warning. It's up to you to decide whether the operation is valid in the context in which it occurred.

The alert looks something like this:

VIRUS-LIKE ACTIVITY: The NEWGAME is attempting to write to IO.SYS.

To resolve a virus-like activity alert, do one of the following:

- Type C for Continue if the message describes a valid activity for the application you are running.
For example, if you're updating an application and the alert warns you of an attempt to write to a file, the activity is valid.

- Type S for Stop if the detected activity isn't related to what you are trying to do.

For example, if you are playing a game and the alert warns you of an attempt to write to hard disk boot records, the activity is invalid.

What to do if Norton AntiVirus can't repair

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

Do one of the following:

- Update your virus protection and scan again. See [page 37](#) for details.
- Read the information on your screen carefully to identify the type of item that can't be repaired, then match it to one of the types below:
 - Infected files are those with filenames that include .COM or .EXE. Document files such as .DOC, .DOT, and .XLS can also be infected.
 - Compressed files may contain many files. You can often tell a compressed file by its name. Many compressed files end in .ZIP.
 - Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files are replaced using the Rescue Disks or, sometimes, your operating system (Windows or DOS) disks.

Infected files

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

If Norton AntiVirus can't repair a file:

Do one of the following:

- Choose Quarantine.

After the file is quarantined, you can update your virus definitions and scan again or submit the file to SARC for analysis. For more information, see "[Quarantine infected or suspicious files](#)" on page 24

and “Submit a potentially infected file to SARC for analysis” on page 25.

- Choose Delete.

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

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

Compressed files

A compressed file may contain many individual files. For example, MYFILE.ZIP may contain the files: FILE1.DOC, FILE2.DOC, FILE3.TXT, FILE.EXE, and so on. Norton AntiVirus can detect viruses in the individual files within the compressed file. However it cannot repair or delete these files until you uncompress (open up) the compressed file.

To uncompress and repair:

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

- 13 Double-click the Norton AntiVirus Auto-Protect icon in the lower-right corner of the taskbar on your Windows desktop
- 14 Click the Enable button to turn Auto-Protect on again.

Hard disk master boot record or boot record

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

If Norton AntiVirus can't repair your hard disk or master boot record, you can use your up-to-date Norton Rescue Boot Disk to restore it. See "Restoring your hard disk" on [page 36](#) for details.

Floppy disk boot record

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

System file

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

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

Using Rescue Disks in virus emergencies

WHY? Sometimes a virus infection prevents your computer from starting normally. Some viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus alert will tell you when to use your rescue disk set.

To use your Norton AntiVirus rescue disks:

- 1 If your computer is running, choose Shutdown from the Windows Start menu, then switch off your computer using the power switch.
- 2 Place your write-protected Norton Rescue Boot Disk in the A: drive, then switch on your computer.
Slide open the plastic tab on the back of the disk to write-protect it. This prevents a virus from accidentally changing the data stored on the disks.
- 3 After your computer starts, remove the Norton Rescue Boot Disk and insert the Norton AntiVirus Program Disk in the A: drive.
- 4 At the DOS prompt (A:\>), type `GO` and press Enter.
After a few moments Norton AntiVirus will start.
- 5 Follow the on-screen directions.
You are prompted when it's time to insert the Norton AntiVirus Definitions Disk.

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

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

Restoring your hard disk

WHY? There are a few situations in which the master boot record and boot records on your hard disk are damaged by a virus and cannot be repaired.

What to do first

You first need to determine whether the Norton Rescue Boot Disk in your Rescue Disk set is current. This means that you've created a new copy of the Norton Rescue Boot Disk since you last did one or more of the following:

- Added, modified, or removed internal hardware
- Added or removed hard drive partitions
- Upgraded your operating system

Caution: If the critical information stored on the Norton Rescue Boot Disk is outdated, it could cause problems when you attempt to restore your computer. It is unlikely you would be able to fix these problems on your own. However, if you have a current Norton Rescue Boot Disk, the following procedure is safe to attempt.

To restore your hard disk:

- 1 Switch off your computer using the power switch.
- 2 Place your write-protected Norton Rescue Boot Disk in the A: drive, then switch on your computer.
- 3 At the DOS prompt (A:\>), type `RESCUE /RESTORE` and press Enter.

The Restore Rescue Information dialog box appears.

- 4 Make sure Drive A: is specified for the location of the rescue data.
- 5 Check all the items in the Items To Restore group box.
Press Tab to move around the dialog box. Press Spacebar to check or uncheck items.
- 6 Choose Restore to restore the selected items.
- 7 When the process is complete, remove your Norton Rescue Boot Disk from Drive A: and restart your computer.

Keeping virus protection current

WHY? Norton AntiVirus relies on up-to-date information to detect and eliminate viruses. One of the most common reasons you may have a virus problem is that you have not updated your protection files since you purchased the product. Symantec provides online access to these new virus definitions files.

How to update virus protection

You need to update your virus definitions files at least monthly.

- From Windows, use a modem or Internet connection to let LiveUpdate automatically download and install updated files.

The last step in updating virus protection is to update your Norton AntiVirus rescue disks. For details, see [page 40](#).

Updating virus protection with LiveUpdate

WHY? LiveUpdate is the easiest way to keep virus protection current because it automatically downloads the proper files and installs them on your computer. You can get virus protection updates anytime by clicking the LiveUpdate button.



To update virus protection:

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

We recommend Find Device Automatically. However, you may want to control the choice depending on long-distance telephone charges for the direct modem connection or access time from the Internet site.

- 4 Click Next to start the automatic update.

Using LiveUpdate Email

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

To receive LiveUpdate Email:

- 1 From your Internet browser go to <http://www.symantec.com/avcenter/newsletter.html>
- 2 Fill out the registration form.
- 3 Click the Subscribe Me button.

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

To start a LiveUpdate session from the LiveUpdate Email:

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

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

Scheduling automatic LiveUpdates

WHY? Scheduling a LiveUpdate to run automatically is the best way to ensure that you don't forget to update virus protection regularly.

Note: Norton AntiVirus for Windows 98 and Windows 95 use different schedulers. The Windows 98 version uses the new built-in Windows scheduler, while the Windows 95 version uses the Norton Program Scheduler.

To schedule automatic LiveUpdates for Windows 98:

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

To schedule automatic LiveUpdates for Windows 95:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window, click Scheduler.
- 3 Click Add.
- 4 Select Scheduled LiveUpdate for the Type Of Event.
- 5 Select Monthly for the Frequency.
- 6 Click OK to close the dialog box, then click OK again to confirm.
- 7 Click the Exit button in the upper-right corner of the Norton Scheduler dialog box, then click Minimize to close the dialog box but leave the Norton Scheduler running.

Your computer must be turned on and Norton Scheduler must be running when the LiveUpdate is due to take place.

Updating virus protection without LiveUpdate

WHY? Symantec supplies a special program called Intelligent Updater if you cannot use LiveUpdate. You may also choose to download the updates from an online service or bulletin board.

To install the latest virus definitions:

- 1 Do one of the following:
 - Download the Intelligent Updater program to any folder on your computer.
 - Insert the disk you received from Symantec in the A: drive.
- 2 From a My Computer or Windows Explorer window, locate and then double-click the Intelligent Updater program.
- 3 Follow all prompts displayed by the update program.

The Intelligent Updater program searches your computer for Norton AntiVirus, then installs the new virus definitions files in the proper folder automatically.

- 4 Restart your computer.
- 5 Scan your disks to make sure newly discovered viruses are detected.

Updating your Norton AntiVirus rescue disks

It is very important to update your Norton AntiVirus rescue disks every time you receive updated virus definitions files from Symantec. If you did not create rescue disks during install, you can do it now.

WHY? If Norton AntiVirus stops your computer because it finds a virus in memory or for some other serious reason, it may not find or fix the problem unless the latest virus protection files have been copied onto your Norton AntiVirus rescue disks.

See “[Update your Norton AntiVirus Rescue Disks](#)” on page 23 for directions.

To update or create Rescue Disks:

- 1 On the Windows taskbar, click Start, point to Programs, point to the Norton AntiVirus group, then click Rescue Disk.
- 2 Follow the on-screen instructions.
- 3 Test your Norton Rescue Boot Disk.
See “[Testing the Norton Rescue Boot Disk](#)” on page 12.
- 4 Slide open the plastic tab on the back of each disk to write-protect it.

Troubleshooting

The most common problems that occur when using Norton AntiVirus are listed below.

My Norton Rescue Boot Disk doesn't work.

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

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

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

- Start up from your hard disk, insert your Norton Rescue Boot Disk in the A: drive, and, from a DOS prompt, type `SYS A:` and press Enter. This transfers the operating system to the rescue disk. Be sure to retest your Norton Rescue Boot Disk.

I can't boot from my A: drive.

There are three likely reasons for this:

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

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

Complete these steps to change the setting:

- a Reboot your computer.

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

Press if you want to run SETUP.

- b Press the key or keys to launch the Setup program.
- c Set the Boot Sequence to A: C:.

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

- d Save the changes, then exit the Setup program.
- You need to use a special Boot Disk to start your computer. In this case, use the boot disk or startup disk that came with your computer.
 - Your computer is set up with more than one operating system, such as Windows NT and Windows 95. See ["My Norton Rescue Boot Disk doesn't work."](#) on page 41 for more information.

Norton AntiVirus Auto-Protect doesn't load when I start my computer.



If the Norton AntiVirus Auto-Protect icon does not appear in the lower-right corner of the taskbar on your Windows desktop, Auto-Protect is not loaded. There are two likely reasons this is happening:

- You started Windows in SAFE mode. Windows restarts in SAFE mode if the previous Shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down from the Windows Start menu.

Choose Shut Down from the Windows Start menu, select the Restart The Computer option, then click OK.

- Norton AntiVirus is not configured to start Auto-Protect automatically.
 - a Start Norton AntiVirus.

- b Click the Options button in the Norton AntiVirus main window.
- c Click the Auto-Protect tab.
- d Check the Load Auto-Protect At Startup check box.
- e Click OK to save your settings and close the Options dialog box.

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

There are two reasons a virus may continue to infect files:

- The virus may be in a program file with an unusual extension that Norton AntiVirus isn't set to look for. Do this:
 - a Start Norton AntiVirus.
 - b Click the Options button in the Norton AntiVirus main window.
 - c Click the Scanner tab.
 - d Select the All Files option in the What To Scan group.
 - e Click OK to save your settings and close the Options dialog box.
 - f Scan all disks that you use and repair all infected files.
- The source of the infection is a floppy disk. Scan all the floppy disks you use for viruses.

Norton AntiVirus can't repair my infected files.

The main reason that Norton AntiVirus may not be able to repair your infected files is you don't have the latest virus definitions files installed on your computer. You should update these files regularly to protect your computer from the latest viruses. To update virus definitions, see [page 37](#).

Some Norton AntiVirus features are password-protected, and I don't know the password.

Do one of the following:

- Contact your system administrator.
- Uninstall Norton AntiVirus, then reinstall it.

Command-line switches

NAVW32.EXE, the Windows 95/98 scanner, can be run with command-line switches to override configuration settings. When scanning using command-line switches, Norton AntiVirus runs minimized, but will pop open on your screen if a virus is found.

Some switches are used alone, while others are followed by a parameter, either a plus (+) or minus (-) sign. You can use more than one switch and more than one parameter on a command line. The vertical bar symbol (|) means that you should use either parameter, but not both. Do not type the brackets around the parameters on the command line. Use the following syntax to run NAVW32 with switches:

```
NAVW32 [[pathname] options]
```

pathname	Any drive, folder, file, or combination of these is scanned. If you want to scan a combination of items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files (for example, NAVW32 A: C:\MYDIR*.EXE).
/A	All drives, except drives A: and B:, are scanned. Network drives are scanned if the Allow Network Scanning option is selected in the Scanner Advanced Settings dialog box.
/L	All local drives, except drives A: and B:, are scanned.
/S[+ -]	All subfolders of any folders specified in the pathname are also scanned.
/M[+ -]	Enables (+) or disables (-) scanning of memory (for example, NAVW32 C: /M+ or NAVW32 D: /M-).
/MEM	Only memory is scanned.
/B[+ -]	Enables (+) or disables (-) scanning of boot records (for example, NAVW32 A: /B+ or NAVW32 B: /B-).
/BOOT	Only the boot records of the specified drives are scanned.
/NORESULTS	No scan results are reported on screen. Used for scheduled or unattended scans.

Examples of usage

- To scan all .EXE files in your GAMES folder, type:
`NAVW32 C:\GAMES*.EXE`
- To scan the GAMES folder on your hard disk, your D: drive, and the file C:\SAMPLES\SAMPLE.EXE, use the Run command and type the following:
`NAVW32 C:\GAMES D: C:\SAMPLES\SAMPLE.EXE`
If C:\SAMPLES is the current folder, type:
`NAVW32 C:\GAMES D: SAMPLE.EXE`
- To scan a folder on the network drive P: called PROGRAMS and all of its subfolders, type:
`NAVW32 P:\PROGRAMS /S`
- To scan memory only, type:
`NAVW32 /MEM`
- To scan only the boot records of drives C: and A: type:
`NAVW32 C: A: /BOOT`
- To specify paths with long filenames that contain spaces, use double quotes:
`NAVW32 "C:\Homework Helper"`

Potential Virus Submission Procedure

If you suspect your system has been infected by an unknown virus, complete the requested information on this form. Then follow the procedure on the back of the form to create a "virus sample" floppy disk. Send the form and the floppy disk to Symantec at the address below. The Symantec AntiVirus Research Center will analyze your disk and inform you of the results. This is a free service provided to Norton AntiVirus customers as part of Symantec's commitment to virus-free computing.

Symantec AntiVirus Research Center

2500 Broadway, Suite 200

Santa Monica, CA 90404

Do *not* write "Contains Live Virus" on the envelope or disk mailer (this upsets the post office). All disks become property of Symantec and will be destroyed.

Please provide the following information:

Operating System:

☐ DOS (version _____) ☐ Windows 95/98 ☐ Windows NT ☐ Windows 3.x

Have you loaded the most recent virus definitions?

☐ Yes (date of VIRSCAN.INF file _____) ☐ No (date of VIRSCAN.INF file _____)

Has any other scanner identified a virus?

☐ Yes (name and version of scanner _____ virus reported _____) ☐ No

Describe the observed virus behavior with as much detail as possible (include infected products, versions, and component information):

Your Name _____

Company Name _____

Street Address _____

City _____ State _____ Zip/Postal Code _____

Country _____ Daytime Phone _____

Fax _____ Email Address _____

Creating a Virus Sample Floppy Disk

If Norton AntiVirus reports that a file is infected with an unknown virus, or if you suspect that a program or document is infected, you can send it to the Symantec AntiVirus Research Center (SARC) for analysis.

Note: For Windows 95/98 and Windows NT, you can Quarantine a suspicious file and send it to SARC via the Internet for analysis. For more information, see "Submitting a file to SARC for analysis" in this guide.

Have you updated your virus definitions file to the most recent version? See "Keeping virus protection current" in this guide for directions to receive the most recent virus definitions file. Then scan again. If you still think you have an unknown virus infection, use the following procedure to create a "virus sample" floppy disk. The Symantec AntiVirus Research Center (SARC) will examine the disk and contact you with the results. This is a free service provided to Norton AntiVirus users.

To create a virus sample floppy disk:

- 1 Start the potentially infected system from its own hard drive.
Windows 95/98: Press function key F8 before Windows starts and choose "Safe mode command prompt only" from the on-screen menu.
- 2 Format a floppy disk with the potentially infected operating system.
From the DOS prompt, type `FORMAT A: /S` and press Enter.
- 3 Do one of the following:
 - Windows 3.1/DOS: Copy MODE.COM, MEM.EXE, KEYB.COM, and XCOPY.EXE from your C:\DOS folder to the floppy disk.
 - Windows 95/98: Copy MODE.COM, MEM.EXE, KEYB.COM, and XCOPY.EXE from your C:\WINDOWS\COMMAND folder to the floppy disk.
 - Windows NT: Copy COMMAND.COM, CMD.EXE, MODE.COM, MEM.EXE, and MORE.EXE from \Winnt\system32 to the floppy disk.
- 4 Type `A:` and press Enter to change to the A: drive.
- 5 Type `PATH;` and press Enter (don't forget the semicolon) to remove the path from the environment temporarily.
- 6 Run the programs (ignore any screen messages). The engineers will be able to determine if they become infected. For example,
 - Type `A:MODE` and press Enter.
 - Type `A:MEM` and press Enter.
 - Type `A:XCOPY` and press Enter.
- 7 Program viruses: Copy any files that you suspect are infected to the floppy disk in the A: drive.
Word macro viruses: Copy any documents that you suspect are infected, along with NORMAL.DOT from the TEMPLATE directory, to the floppy disk in the A: drive.
Excel macro viruses: Copy any worksheets that you suspect are infected, along with any files in the XLSTART directory, to the floppy disk in the A: drive..
- 8 Label the floppy disk with your name, address, telephone number, and the date of its creation. Write "Potential Virus" on the disk label.
- 9 Complete and send the form on the previous page with the floppy disk to Symantec.

I N D E X

Symbols

- " (double quotes), 45
- (minus sign), 44
- + (plus sign), 44
- ., 41
- | (vertical bar), 44

A

- alerts
 - Windows 95/98, 27, 28–31
- applications
 - See also* software
 - virus-like activity, valid vs. invalid, 30–31
- Auto-Protect feature
 - See also* virus protection
 - disabling temporarily
 - Windows 95/98, 18, 33
 - enabling
 - Windows 95/98, 18, 34, 42
 - failure to load on startup
 - Windows 95/98, 42–43
- Auto-Protect icon
 - Windows 95/98, 17, 18

B

- backup copies
 - infected, 28, 33
 - replacing deleted infected files, 33
 - software purchases, 17
- boot records
 - hard disk. *See* master boot record
 - scanning only, 44, 45
 - unable to repair
 - Windows 95/98, 34

booting

- Auto-Protect failure to load after, 42–43
- floppy drive not set for
 - Windows 95/98, 41

C

CD

- installing Norton AntiVirus
 - Windows 95/98, 10
- command-line switches, scanner
 - Windows 95/98, 44
- compressed files
 - file extension, 32
 - repairing
 - Windows 95/98, 33
 - scanning downloaded
 - Windows 95/98, 16
- computer system
 - behavior of viruses in
 - Windows 95/98, 15
- Continue action button
 - Windows 95/98, 28, 30
- customizing
 - Norton AntiVirus
 - Windows 95/98, 24

D

- decompressing files. *See* uncompressing
 - files for repair
- Delete action button
 - Windows 95/98, 28
- deleting infected files
 - See also* removing viruses
 - procedure
 - Windows 95/98, 32–33
 - when and why
 - Windows 95/98, 28

- directories
 - See also* folders
- disabling
 - virus protection
 - Windows 95/98, 18, 33
- disk space requirements for Norton AntiVirus
 - for Windows 95/98, 9
- documentation. *See* online documentation
- DOS. *See* Norton AntiVirus for DOS; Norton AntiVirus for Windows 3.x/DOS
- double quotes ("), 45
- downloads
 - scanning automatically, 16
 - virus protection during
 - automatic scanning, 16
 - Netscape plug-ins, 11
- drives, scanning
 - Windows 95/98, 21, 44

E

- enabling virus protection
 - Windows 95/98, 16, 34, 42
- Exclude action button
 - Windows 95/98, 28
- extracting archives. *See* uncompressing files for repair

F

- file extensions
 - infected files, 32
 - scans missing unusual, 43
- files
 - See also* infected files; repairing infected files
 - reinfected after virus removal
 - Windows 95/98, 43
 - scanning individual
 - Windows 95/98, 22, 44, 45
- Find Device Automatically option
 - Windows 95/98, 38

- floppy disks
 - installing Norton AntiVirus
 - Windows 95/98, 10
 - scanning
 - Windows 95/98, 21
 - unable to repair boot record
 - Windows 95/98, 34
- floppy drives, unable to boot from, 41
- folders
 - See also* directories
 - Norton AntiVirus installation default
 - Windows 95/98, 11
 - scanning individual
 - Windows 95/98, 22, 44, 45

H

- hard disk
 - See also* master boot record
 - Rescue Disk updates on repartitioning, 23
 - restoring
 - Windows 95/98, 36
- hardware
 - Rescue Disk updates on changing
 - Windows 95/98, 23
- help. *See* online help

I

- infected files
 - See also* repairing infected files
 - reinfected
 - Windows 95/98, 43
 - types of file extensions, 32
 - unable to repair
 - Windows 95/98, 32–36, 43
- inoculation change alerts
 - Windows 95/98, 30
- inoculation changes, expected vs. unexpected
 - Windows 95/98, 28

installing

- Norton AntiVirus for Windows 95/98
 - configuration options, 10
 - procedure, 10
 - system requirements, 9
- software programs, disabling
 - Auto-Protect, 18
- updated virus definitions
 - Windows 95/98, 39

Intelligent Updater

- Windows 95/98, 39–40

Internet

- See also* downloads; LiveUpdates
- obtaining LiveUpdates
 - Windows 95/98, 37
- protection from viruses on
 - Auto-Protect, 16
 - Netscape plug-ins, 11

L

LiveUpdates

- obtaining
 - Norton AntiVirus installation process, 11
 - when unable to repair files, 32
 - Windows 95/98 procedure, 37–39
- scheduling
 - Windows 95/98, 38
- updating virus protection without
 - Windows 95/98, 39–40

M

master boot record

- Windows 95/98, 34, 36

memory

- removing viruses from
 - Windows 95/98, 29
- scanning, Windows 95/98, 44, 45

messages. *See* alerts

minus sign (-), 44

modem, obtaining LiveUpdates

- Windows 95/98, 37

N

NAVW32.EXE command-line switches, 44–45

Netscape plug-ins

- Windows 95/98, 11

Norton AntiVirus for Windows 95/98

- about, 16
- automatic features, 16
- customizing, 24
- installing
 - configuration options, 10
 - options, 10
 - procedure, 10
 - system requirements, 9
- starting, 20
- uninstalling, 13

Norton AntiVirus window

- Windows 95/98, 20

Norton Rescue Disks, 45

Rescue Disks, 45

O

online help, Norton AntiVirus

- Windows 95/98, 21

opening Norton AntiVirus window

- Windows 95/98, 20

operating systems

- multiple installed
 - Windows 95/98, 41
- Rescue Disk updates on changing
 - Windows 95/98, 23

P

password-protected features inaccessible

- Windows 95/98, 43

pathnames, scanner command line, 44

plus sign (+), 44

Problems Found dialog

- Windows 95/98, 27

programs. *See* applications; software

Q

- Quarantine in Norton AntiVirus
 - for Windows 95/98, 24
 - put a file in, 24
 - rescan a file, 24
- quotes, double ("), 45

R

- record, 34
- removing viruses
 - See also* repairing infected files
 - deleting infected files
 - Windows 95/98, 32–33
 - from memory
 - Windows 95/98, 29
- Repair action button
 - Windows 95/98, 28
- Repair Wizard
 - Windows 95/98, 27
- repairing infected files
 - See also* removing viruses
 - compressed
 - Windows 95/98, 33
 - Repair action button
 - Windows 95/98, 28
 - unsuccessful
 - Windows 95/98, 32–36, 43
- Rescue Disks, 45
 - creating
 - Windows 95/98, 10, 12, 19, 40
 - updating, 23, 40
 - Windows 3.x/DOS. *See* Norton Rescue Disks
- restoring hard disk
 - Windows 95/98, 36

S

- scanners
 - command-line switches
 - Windows 95/98, 44–45
- scanning
 - all files
 - Windows 95/98, 43
 - drives
 - Windows 95/98, 21
 - individual items
 - Windows 95/98, 22, 44, 45
 - installation options
 - Windows 95/98, 11
 - memory, 44, 45
- scans
 - scheduling
 - Windows 95/98, 22–23
- scheduling
 - LiveUpdates
 - Windows 95/98, 38
 - scans
 - Windows 95/98, 22–23
- Setup program, changing drive boot sequence
 - Windows 95/98, 42
- software
 - See also* applications
 - avoiding infected
 - Windows 95/98, 17
 - disabling virus protection when installing
 - Windows 95/98, 18
- Start menu, accessing Norton AntiVirus
 - Windows 95/98, 20
- starting
 - Norton AntiVirus
 - Windows 95/98, 20
- Stop action button
 - Windows 95/98, 28, 31
- Symantec AntiVirus Research Center
 - submit a file to, 25
- system files
 - changes to
 - inoculation change alerts, 30
 - unable to repair
 - Windows 95/98, 34, 43
- system messages. *See* alerts

T

turning off. *See* disabling

U

uncompressing files for repair

Windows 95/98, 33

uninstalling Norton AntiVirus

Windows 95/98, 13

unzipping files. *See* uncompressing files for repair

updating

Rescue Disks

Windows 95/98, 23, 40

virus protection

Windows 95/98, 16, 37

without LiveUpdate, 39–40

V

vertical bar (|), 44

virus alerts

Windows 95/98, 27, 28–31

virus definitions

See also LiveUpdates; virus protection,

updating

adding updates to Rescue Disks, 40

installing latest, 39

updating

recommended frequency, 17

virus protection

disabling

Windows 95/98, 18, 33

enabling

Windows 95/98, 18, 34, 42

keeping current

Windows 95/98, 37–40

Norton AntiVirus features

Windows 95/98, 16

updating

See also LiveUpdates

without LiveUpdate, 39–40

user responsibilities

Windows 95/98, 16

viruses

See also removing viruses

avoiding

Windows 95/98, 17

behavior, 15

constant release of new, 16

detected. *See* virus alerts

virus-like activity alerts

Windows 95/98, 30–31

W

WHY, 12

Windows 95/98

irreparable system files, 34

SAFE mode, 42