

Norton AntiVirus™ User's Guide

Norton
AntiVirus 2001™

Norton AntiVirus™ 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 © 1995-2001 Symantec Corporation. All Rights Reserved.

Documentation version 7.20

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 changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Norton, Norton SystemWorks, Emergency Disk, LiveUpdate, Norton AntiVirus, and Norton Utilities are trademarks of Symantec Corporation.

Windows is a registered trademark of Microsoft Corporation. AOL and CompuServe are registered trademarks of America Online, Inc. Prodigy Internet is a trademark of Prodigy. Pentium is a registered trademark of Intel Corporation. Other product names mentioned in this manual may be 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 accompanying software to you only upon the condition that you accept all of the terms contained in this license agreement. Please read the terms carefully before continuing installation, as pressing the "Yes" button will indicate your assent to them. If you do not agree to these terms, please press the "No" button to exit install as Symantec is unwilling to license the software to you, in which event you should return the full product with proof of purchase to the dealer from whom it was acquired within sixty days of purchase, and your money will be refunded.

LICENSE AND WARRANTY:

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

YOU MAY:

- (i) use one copy of the Software on a single computer;
- (ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
- (iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
- (iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
- (v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

YOU MAY NOT:

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

SIXTY DAY MONEY BACK GUARANTEE:

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

LIMITED WARRANTY:

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

The above warranty is exclusive and in lieu of all other warranties, whether express or implied, including the implied warranties of merchantability, fitness for a particular purpose and noninfringement. This warranty gives you specific legal rights. You may have other rights, which vary from state to state.

DISCLAIMER OF DAMAGES:

Regardless of whether any remedy set forth herein fails of its essential purpose, in no event will Symantec be liable to you for any special, consequential, indirect or similar damages, including any lost profits or lost data arising out of the use or inability to use the software even if Symantec has been advised of the possibility of such damages.

Some states do not allow the limitation or exclusion of liability for incidental or consequential damages so the above limitation or exclusion may not apply to you.

In no case shall Symantec's liability exceed the purchase price for the software. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

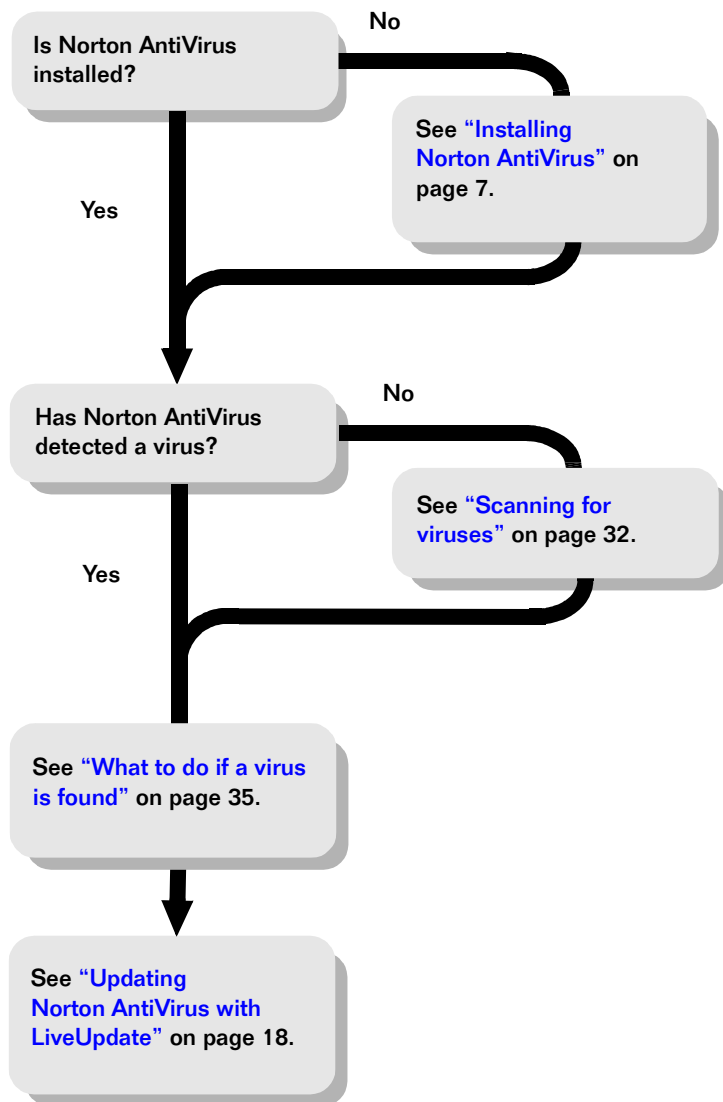
U.S. GOVERNMENT RESTRICTED RIGHTS:

All Symantec products and documentation are commercial in nature. The Software and documentation are "Commercial Items", as that term is defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R. §12.212 and 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

GENERAL:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

Help! I've got a virus.



C O N T E N T S

Chapter 1 Installing Norton AntiVirus

Installing Norton AntiVirus	7
System requirements	7
Email programs	8
Emergency procedures	8
Installation procedure	10
Keeping your system protected	10
Automatic LiveUpdate	10
LiveUpdate	11
Uninstalling Norton AntiVirus	11

Chapter 2 Introducing Norton AntiVirus

What's new in Norton AntiVirus 2001?	13
Norton AntiVirus	14
Protection from harmful code	14
Detection of viruses in compressed files	14
Email scanning	14
Quarantine	14
Updating with LiveUpdate	15

Chapter 3 Norton AntiVirus basics

Navigating Norton AntiVirus	17
Setting options	18
Updating Norton AntiVirus with LiveUpdate	18
Using help to learn more about Norton AntiVirus	19

Chapter 4 Responding to Norton AntiVirus alerts

Norton AntiVirus alerts	23
-------------------------------	----

Chapter 5 Preventing viruses with Norton AntiVirus

Understanding and avoiding viruses	27
Understanding Trojan Horses	28
Understanding worms	28
What Norton AntiVirus does automatically	28
What you have to do	29
Tips for avoiding viruses	29
Maintaining full-time protection with Auto-Protect	30

Temporarily disabling Auto-Protect	31
Scanning for viruses	32
Protecting your email	32

Chapter 6 Norton AntiVirus emergency procedures

What to do if a virus is found	35
Quick guide to alert actions	35
Types of virus alerts	36
What to do if Norton AntiVirus cannot repair	38
Submitting files to SARC	40

Chapter 7 Troubleshooting

Service and support solutions

CD Replacement Form

Potential Virus Submission Procedure

Index

Installing Norton AntiVirus

Welcome to Norton AntiVirus, the number one antivirus software in the world.

Installing Norton AntiVirus

Before installing Norton AntiVirus, take a moment to review the system requirements listed in this section. You should have some blank floppy disks available to make Emergency Disks.

Note: You do not need to uninstall previous versions of Norton AntiVirus from your system before running Setup, but you should remove any other antivirus software.

System requirements

To use Norton AntiVirus, your computer must meet the following minimum requirements.

Windows 95 OSR2

- Intel 80486DX/66 processor
- 32 MB of memory
- 50 MB of hard disk space
- CD-ROM disk

Email programs

Norton AntiVirus automatically configures the following email clients for email protection:

- Microsoft Outlook Express 4.0/5.x
- Microsoft Outlook 97/98/2000
- Netscape Messenger 4.x
- Eudora Light 3.0
- Eudora Pro 4.0
- Pegasus Mail 3.0
- Becky! Internet Mail 1.26
- Al-Mail 1.11

Norton AntiVirus can protect other POP3 clients, but you must manually configure the client for protection. See Help for more information.

Emergency procedures

When you install Norton AntiVirus, it scans for viruses in memory. If it finds an active virus, use Emergency Disks to remove the virus before you finish installing.

Make Emergency Disks from the Norton AntiVirus CD to help you recover from the emergency. You will need several formatted 1.44 MB disks.

You can use the CD that contains Norton AntiVirus as an Emergency Disk if your computer can start up from the CD-ROM drive. See [“Using the CD as an Emergency Disk”](#) on page 9.

Warning: Perform the following procedure on a different computer from the one with the problem. Executing these steps might cause additional problems.

To make Emergency Disks:

- 1 Insert the Norton AntiVirus CD into the CD-ROM drive.
- 2 Click Browse the CD.
- 3 Double-click the Support folder.
- 4 Double-click the Edisk folder.

- 5 Double-click Ned.exe.
- 6 Follow the on-screen instructions.

To use the Emergency Disks:

- 1 If your computer is running, click the Start button, select Shut Down, and then select the Shut Down option. When Windows has shut down, switch off your computer using the power switch.
- 2 Insert Emergency Disk 1 in your floppy drive, and then switch on your computer.
- 3 Follow the on-screen instructions.

The Emergency program takes several minutes to load, and then it automatically scans your computer and removes viruses.

If you cannot start up from drive A, see [“I cannot start up from my A: drive”](#) on page 44.

Using the CD as an Emergency Disk

You can use the Norton AntiVirus CD as an Emergency Disk if your computer can start up from the CD-ROM drive. Wherever the instructions say to insert Emergency Disk 1 and restart your computer, follow these steps instead.

To use the CD as an Emergency Disk:

- 1 Insert the Norton AntiVirus CD into your CD-ROM drive.
- 2 Restart your computer.

You may need to change your computer's BIOS Setup options to start up from the CD-ROM drive. Refer to your computer manual to see how to change the startup device.

When you are running from the CD, you can skip instructions to insert other Emergency Disks. All the information for all the Emergency Disks is on the CD.

Installation procedure

To install:

- 1 Start Windows (if it is not already running).
- 2 Close all Windows programs to prevent conflicts.
- 3 Insert the Norton AntiVirus CD in the CD-ROM drive. An opening screen appears.
- 4 Click Install Norton AntiVirus and follow the on-screen instructions.
The preselected options in Setup are the correct choices for most people. You should accept the preset choices unless you have a very unusual need.

If the opening screen does not appear:

- 1 Double-click the My Computer icon.
- 2 Double-click the icon for your CD-ROM drive.
- 3 Double-click CDSTART.EXE.
- 4 Click Install Norton AntiVirus and follow the on-screen instructions.

While this user's guide contains helpful information, there is additional information in online help that is not covered here. There is also a wealth of information at <http://service.symantec.com>.

Keeping your system protected

Norton AntiVirus gives you the tools you need to keep your system protected.

Automatic LiveUpdate

Automatic LiveUpdate checks for new virus definitions when you are connected to the Internet. It can update your virus protection without interrupting your work.

LiveUpdate

The LiveUpdate button at the top of the main screen updates your virus protection and Norton AntiVirus programs. See [“Updating Norton AntiVirus with LiveUpdate”](#) on page 18.

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 virus protection since you purchased the product. You should update your virus protection at least once a week.

Uninstalling Norton AntiVirus

You can easily remove Norton AntiVirus from your computer.

To remove Norton AntiVirus from your computer:

- 1 Click the Start button, and then select Settings > Control Panel.
- 2 Double-click Add/Remove Programs.
- 3 In the list of installed programs, select Norton AntiVirus. Click Add/Remove.
- 4 Follow the on-screen instructions.

You might also want to uninstall LiveUpdate and LiveReg if you have no other Symantec products installed.

Introducing Norton AntiVirus

Norton AntiVirus automatically protects against all viruses and Trojan horses, plus it protects you against malicious ActiveX and Java applets. It quarantines infected files before they damage your system and provides help with suspected infections directly from Symantec researchers. Norton AntiVirus automatically updates virus definitions with LiveUpdate.

What's new in Norton AntiVirus 2001?

Automatic LiveUpdate checks for new virus definitions when you are connected to the Internet. It can update your virus protection without interrupting your work.

SmartScan improves file scanning performance and reduces system impact from constant background monitoring for viruses. SmartScan determines what files contain executable code, and then it scans only those files for viruses and other malicious code.

SmartScan represents a significant security enhancement for users who scan program files and documents only. SmartScan looks into every file to determine if there is executable code and it ensures that no files that might contain viruses escape the scanning engine.

Comprehensive email scanning protection provides added support for clients with Secure Password Authentication such as MSN. Norton AntiVirus scans email automatically as it is received from the server and detects viruses lurking in email attachments before you even save or launch the attachment, eliminating the risk of unknowingly forwarding viruses to third parties.

A new email status window lists what email accounts you have and whether email protection is enabled for those accounts. It makes it easy to configure email antivirus protection.

The bootable CD provides antivirus protection that lets you easily recover from virus emergencies.

Norton AntiVirus

Norton AntiVirus protects you from harmful code that might try to infiltrate your computer. You are safe from infection whether you are receiving email attachments, downloading files from the Internet or from a network, or inserting a floppy disk into your computer.

Protection from harmful code

Norton AntiVirus protects you from malicious code, including viruses, Trojan horses, ActiveX controls, and Java applets so you're safe when you use your computer and when you're on the Internet.

Detection of viruses in compressed files

Norton AntiVirus checks for viruses and other malicious code inside of compressed files, such as .zip files. It can even find and fix problems inside a compressed file that is contained within another compressed file. Protection is not limited to just .zip files; Norton AntiVirus finds problems inside many kinds of compressed files.

Email scanning

Norton AntiVirus checks email attachments as you receive them. If a virus is found, Norton AntiVirus will repair it for you.

Quarantine

When Norton AntiVirus finds a file it can't repair, it safely isolates the file in a Quarantine area. This lets you update your virus protection so that you can fix the problem completely.

Updating with LiveUpdate

LiveUpdate retrieves “micro definitions” that contain just the information you need to update your virus protection. New virus definitions are posted on the Symantec website weekly, so you can update your virus protection every week or allow Norton AntiVirus automatic LiveUpdate to manage updating for you.

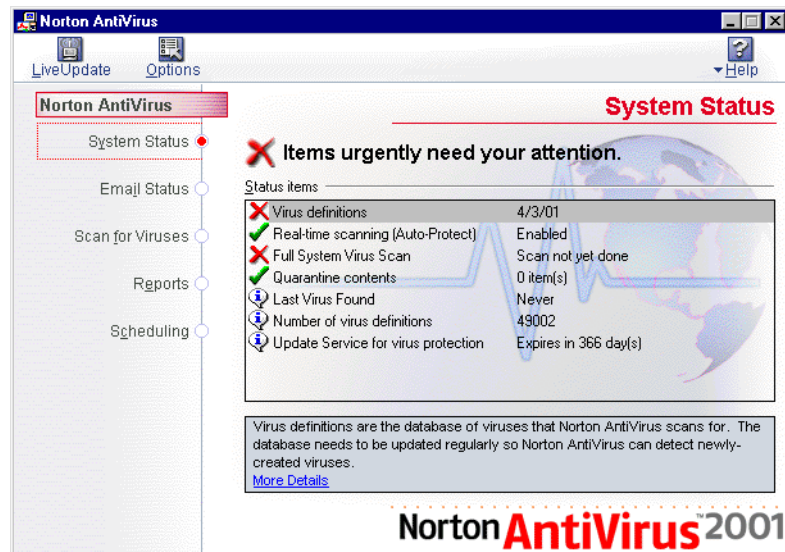
Norton AntiVirus basics

This chapter provides you with the basics of using Norton AntiVirus.

Navigating Norton AntiVirus

To start Norton AntiVirus:

- 1 On the Windows taskbar, click Start > Programs > Norton AntiVirus > Norton AntiVirus 2001.



The Norton AntiVirus main screen is the starting point for all your activities.

- 2 From here you can do the following:
 - Click an option on the left to see a description of what it provides on the right.
 - Click one of the buttons at the top for features that apply to more than one area of the program.

Additional Symantec products might appear if you have them installed.

Setting options

There are many options you can set in Norton AntiVirus. For example, you can choose to scan all files, instead of scanning program files and documents only.

To set options:

- 1 Click the Options button at the top of the Norton AntiVirus main window.
- 2 Choose the feature for which you want to set options.

Updating Norton AntiVirus with LiveUpdate

Click the LiveUpdate button to update Norton AntiVirus programs and virus protection. LiveUpdate connects to Symantec to see if updates are available for Norton AntiVirus and also checks for updates to your virus protection. LiveUpdate requires an Internet connection.

Note: Symantec does not charge for updates to Norton AntiVirus programs, however there is a charge for updating your virus protection after your free subscription expires.

Note: Your normal Internet access fees apply.

To update Norton AntiVirus using LiveUpdate:

- 1 Click the LiveUpdate button at the top of the Norton AntiVirus main window.
- 2 The LiveUpdate window appears. Follow the on-screen instructions.

Tip: If you connect to the Internet through AOL, CompuServe, or Prodigy Internet, first connect to the Internet, and then run LiveUpdate.

Using help to learn more about Norton AntiVirus

Norton AntiVirus provides extensive online help. This help system gives you detailed instructions about how to use all of Norton AntiVirus.

Norton AntiVirus includes three kinds of help:

- Help with program dialog boxes
- How To help
- What's This? help

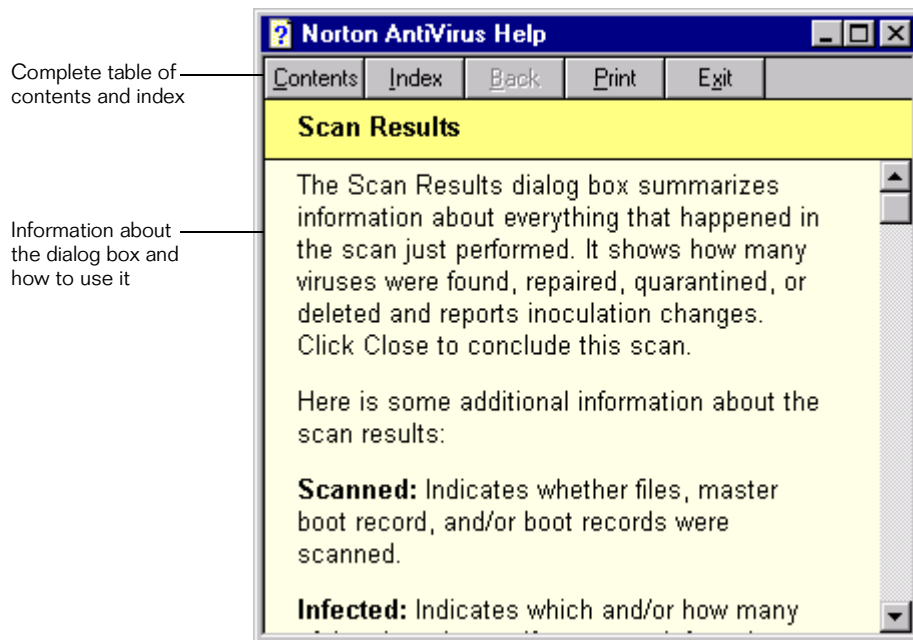
Help with program dialog boxes

The Help dialog box provides information about the area of the program you are using. This kind of help is context-sensitive, meaning that it displays help for the specific dialog box that you are currently using.

To get help with a dialog box:

- Click the Help button located in the dialog box.

A help topic pertaining to the current dialog box appears.



How To help

How To help explains step-by-step procedures you are likely to perform using Norton AntiVirus. You can access these topics through the Contents or Index tabs. Open the Contents and Index by clicking the Help Topics, Contents, or Index button at the top of any help topic.

What's This? help

What's This? help provides a quick definition of an individual component of a window or dialog box.

To access What's This? help:

- Right-click anywhere you need help in a window or dialog box and choose What's This?

Getting help from the Help menu

Help is always available from the Norton AntiVirus main window.

To access the Help menu:

- Click Help at the top of the main Norton AntiVirus window.



Responding to Norton AntiVirus alerts

When Norton AntiVirus detects a problem with your system it displays a message on your screen. These messages, called alerts, take several forms. These alerts may appear when you are running other programs and Norton AntiVirus detects a problem. This chapter shows examples of the various types of alerts that you may see, and tells you what actions you should take to respond to them.

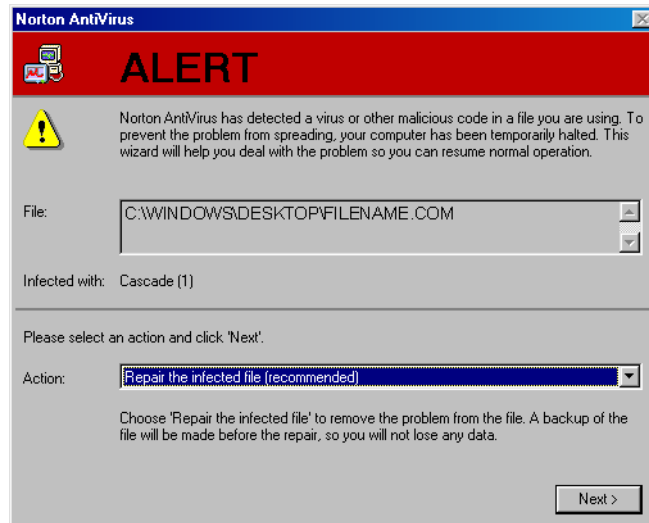
Norton AntiVirus alerts

Norton AntiVirus displays different alerts, depending on when it finds a virus or notices virus-like activity.

Virus Alerts

These messages appear when Norton AntiVirus detects viruses, Trojan horses, and other types of malicious code.

If you see this type of alert:



- Click Next. The wizard will help you fix the problem.

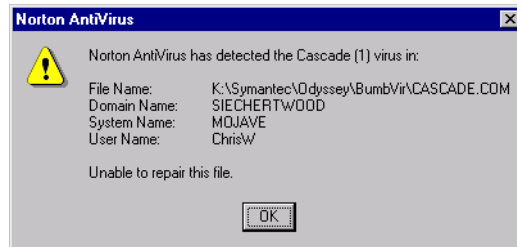
If you see this type of alert:



- 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.

For more information, find the type of problem in [“Types of virus alerts”](#) on page 36. For example, if the message says VIRUS IN MEMORY, look for “VIRUS IN MEMORY.”

If you see an alert like this:



- 1 Click OK (possibly several times).
- 2 Scan your disk to eliminate the virus. See [“Scanning for viruses”](#) on page 32.

Preventing viruses with Norton AntiVirus

Understanding and avoiding viruses

A computer virus is 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 is 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 drive.
- Remain inactive until a predetermined trigger date (for example, Friday the 13th) to wreak havoc.

What viruses do not 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 is stored on them.

Understanding Trojan Horses

A Trojan Horse, while not technically a virus, has the potential to cause the same kinds of problems that viruses do. Many Trojan Horses are designed to steal your login ID and password and then email them to someone else who can make use of the account at your expense. Other Trojan Horses display obscene messages or delete the contents of your hard drive.

You typically get Trojan Horses by downloading a program that seems safe or promises something like free online time. Once it is downloaded and executed, the malicious code begins to work. The difference between Trojan Horses and viruses is that Trojan Horses do not replicate or spread on their own. They can only be transmitted intentionally via email or disk, or downloaded directly onto a PC. This means that, unlike a virus, you are typically only affected once by a specific Trojan Horse.

Understanding worms

Like viruses, worms replicate themselves. However, instead of spreading from file to file they spread from computer to computer, infecting an entire system.

Worms copy themselves from one computer to another over a network (using e-mail, for example). Because worms don't require human interaction to replicate, they can spread much more rapidly than computer viruses.

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. Norton AntiVirus protects your computer in the following ways:

- Eliminates viruses and repairs files.
- Makes sure your computer is safe from viruses at startup.
- Checks for viruses every time you use programs on your computer, floppy disks, and document files that you receive or create.
- Checks for viruses in email attachments each time you receive email from the Internet.

- 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 drives are virus-free. Even files within compressed files are scanned.
- Provides complete protection from Internet-borne viruses. No separate programs or Norton AntiVirus options changes are necessary. Auto-Protect scans program and document files automatically as they are downloaded.
- When Automatic LiveUpdate is enabled, Norton AntiVirus checks for, and installs, updated virus protection when you are connected to the Internet.

What you have to do

New viruses are being written all the time so you have to regularly update your virus protection. If you do not, you are not protected against viruses that have been released into the computer world since you bought the product.

Keep your virus protection up-to-date. Automatic LiveUpdate does this for you automatically. Or, you can update your protection at any time with LiveUpdate. To update virus protection, see [“Updating Norton AntiVirus with LiveUpdate”](#) on page 18.

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 enabled at all times. You can also start Norton AntiVirus and check that Real-time scanning (Auto-Protect) is enabled.
- Regularly update your virus protection from Symantec to keep up with the new viruses that have been released since you installed Norton AntiVirus.
- Be cautious about unexpected email and email with attachments that might contain a virus.

- 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 [“Scanning for viruses”](#) on page 32.

Maintaining full-time protection with Auto-Protect

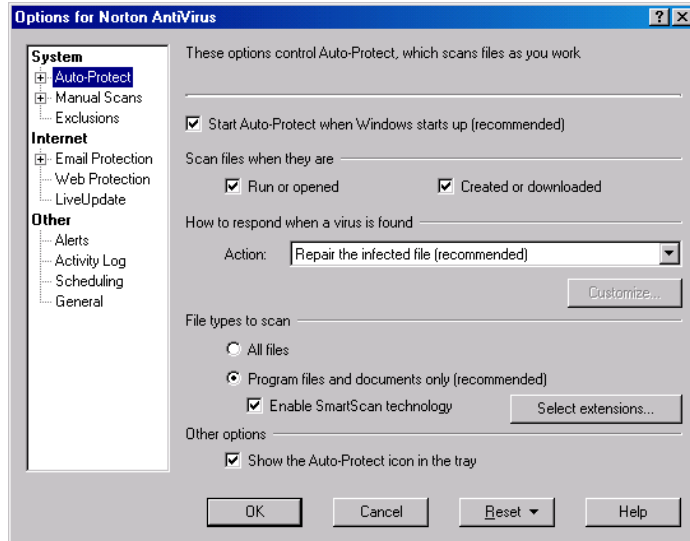
Norton AntiVirus is preset to provide you with complete protection against viruses. It is unlikely you need to change any settings. However, you can ensure that Auto-Protect is working by following these steps.

To ensure that Auto-Protect is enabled:

- 1 Start Norton AntiVirus.
- 2 Check that it says that Real-time scanning (Auto-Protect) is enabled. If it is disabled, double-click the Real-time scanning (Auto-Protect) line and click Yes.
- 3 Click the Options button at the top of the Norton AntiVirus main window.
- 4 Click Auto-Protect in the list on the left.

- 5 Be sure that Start Auto-Protect When Windows Starts Up is checked.

Tip: For maximum protection, your Auto-Protect options should be set as shown below.



Temporarily disabling Auto-Protect

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

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

To turn off Norton AntiVirus Auto-Protect temporarily:

- Right-click the Norton AntiVirus Auto-Protect icon on the taskbar in the lower-right corner of your Windows desktop, and then click Disable Auto-Protect.

To turn on Norton AntiVirus Auto-Protect:

- Right-click the Norton AntiVirus Auto-Protect icon on the taskbar in the lower-right corner of your Windows desktop, and then click Enable Auto-Protect.

Scanning for viruses

You should scan all floppy disks for viruses before you use them.

To scan drives for viruses:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window, click Scan For Viruses.
- 3 Select the item you want to scan from the list.
If what you want to scan is not in the list, click Add Scan to start the Scan Wizard, which will help you build a custom scan.
- 4 Click Run Scan Now.

To quickly scan a drive, folder, or file, right-click an item in My Computer or Windows Explorer and choose Scan With Norton AntiVirus.

Protecting your email

Norton AntiVirus scans your email by intercepting it before it reaches your email program. It does this by modifying the user name and server name in your email client program. The server name is changed to Pop3.norton.antivirus, and the user name is changed to a combination of your user name and email server name. See help for details about these settings, as well as how to configure a POP3 email client that Norton AntiVirus does not recognize.

When Norton AntiVirus is scanning incoming email, the email scanning icon appears in the notification area of the Windows taskbar.

When you are downloading a large attachment, your email program might display a warning because it is not receiving information fast enough. This is because Norton AntiVirus must check the entire attachment before passing it on to the email client. If you see this kind of a message, you should enable Protect Against Timeouts When Scanning Email.

To ensure that timeout protection is enabled:

- 1** Start Norton AntiVirus.
- 2** At the top of the Norton AntiVirus main window, click the Options button.
- 3** In the list on the left, expand Email Protection.
- 4** Click Advanced.
- 5** Make sure Protect Against Timeouts When Scanning Email is checked.

Norton AntiVirus emergency procedures

What to do if a virus is found


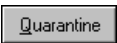
When you see one of the Norton AntiVirus alerts shown in [“Responding to Norton AntiVirus alerts”](#) on page 23, you can use the information in this chapter to help you respond appropriately.





Quick guide to alert actions

Most virus alerts can be handled directly from the alert that appears on your screen. The recommended action is always pre-selected.

If a Norton AntiVirus alert appears on your screen, and you are not sure what option to select, use this table to decide what to do. If you need more information, see [“Types of virus alerts”](#) on page 36 for step-by-step instructions.

In some situations, your mouse will not work when an alert appears. In these cases, press the first letter of your selection (for example, press **R** for Repair) or press Enter to accept the recommended selection.

Actions	When and why you use them
	Eliminates the virus and repairs the infected item. When a virus is found, Repair is always the best choice.
	Isolates the virus-infected file, but does not remove the virus. Select 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.

Actions	When and why you use them
	Erases both the virus and the infected file. The virus and file are gone forever. Select Delete if Repair is not successful. 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 will be alerted again the next time you do the same thing.
	Continues the current operation. Select Continue only if you are sure a virus is not at work. You will be alerted again. If you are not sure what to do, select Stop.
	If you select Exclude and a virus is at work, the virus will not be detected. Exclude should be used only by system administrators for system tuning.

Types of virus alerts

VIRUS FOUND

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

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

To get rid of a virus infection:

- Press R for Repair.

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

If Norton AntiVirus cannot repair the infection, see [“What to do if Norton AntiVirus cannot repair”](#) on page 38.

VIRUS IN MEMORY

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

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

A memory virus warning says similar to this:

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

The computer is halted. Restart from your Emergency Boot Disk, and 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 Emergency Boot Disk into the A: drive.
- 3 After waiting a few seconds, turn the computer on.
- 4 Follow the on-screen directions.

If you cannot start up from the A: drive, see [“I cannot start up from my A: drive”](#) on page 44.

VIRUS-LIKE ACTIVITY

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

The alert looks similar to 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:

- Press **C** for Continue if the message describes a valid activity for the application you are running.

For example, if you are updating an application and the alert warns you of an attempt to write to a file, the activity is valid.

- Press **S** for Stop if the detected activity is not 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 the boot records of your hard drive, the activity is invalid.

What to do if Norton AntiVirus cannot repair

One of the most common reasons Norton AntiVirus cannot repair a file is that you do not have the most up-to-date virus protection. Use LiveUpdate to obtain the latest virus protection.

Do one of the following:

- Update your virus protection and scan again. For details, see [“Updating Norton AntiVirus with LiveUpdate”](#) on page 18.
- Read the information on your screen carefully to identify the type of item that cannot be repaired, and then match it to one of the types below:
 - Infected files are those with filename extensions such as .EXE, .DOC, .DOT, or .XLS. Files with any name can be infected.
 - 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 Emergency Disks or, sometimes, your operating system (Windows or DOS) disks.

Infected files

If infected files cannot 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 spread.

Note: Some infections can be removed by special removal tools that are on the Norton AntiVirus CD in the Support\NAVTools\Repair folder. These tools are also available on the Symantec Web site. Go to <http://www.symantec.com/avcenter/> and see if there is a removal tool available for your problem.

If Norton AntiVirus cannot repair a file:

Do one of the following:

- Select Quarantine (recommended).
After the file is quarantined, you can update your virus definitions and scan again or submit the file to SARC for analysis.
- Select 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.

Hard disk master boot record or boot record

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

If Norton AntiVirus cannot repair your hard drive or master boot record, you can use your Emergency Disks to restore it.

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 Emergency Boot Disk or the Windows Startup Disk.

To use your Emergency Disks:

- 1 If your computer is running, choose Shut Down from the Windows Start menu, and then switch off your computer using the power switch.
- 2 Place your Emergency Boot Disk in the A: drive.

Note: 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 waiting a few seconds, turn your computer on.
- 4 Follow the on-screen directions.
You are prompted when it is time to insert other Emergency Disks.
- 5 When the process is complete, remove the Emergency Disk from the A: drive and restart your computer.

Submitting files to SARC

Even though you performed a virus scan using the latest virus definitions, and Norton AntiVirus did not detect a virus, you suspect that your computer has a virus. Place the suspect file in Quarantine. This ensures that the virus doesn't spread. Then, use Scan and Deliver to submit the file to the Symantec AntiVirus Research Center (SARC).

Follow these steps to submit a sample of the suspected virus to the SARC for testing.

Note: If the file is compressed, for example, a .zip file, you will have to uncompress it before you submit it. Scan and Deliver cannot submit compressed files.

To place a file in Quarantine:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window, click Reports.
- 3 Double-click View and manage the items in Quarantine.
- 4 In Norton AntiVirus Quarantine, click Add Item.
- 5 In the Add to Quarantine dialog box, browse to and select the file that you want to place in Quarantine.
- 6 Click Add.

When the file is placed in Quarantine, it is encrypted, and is no longer a threat to the computer.

To submit a quarantined file to SARC using Scan and Deliver:

- 1 Select the file that you want to submit in the right pane of the Quarantine window.
- 2 Click Submit Item.
- 3 Follow the on-screen instructions.

Troubleshooting

The information in this chapter will help you solve the most frequent problems that you may experience. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site. You can find a troubleshooter, updates, patches, online tutorials, knowledge base articles and virus removal tools. Go to <http://service.symantec.com>.

With your Norton AntiVirus CD you can create Emergency Disks. You can use the Emergency Disks to recover from most common emergencies. See [“To make Emergency Disks:”](#) on page 8.

You can use the CD that contains Norton AntiVirus as an Emergency Disk if your computer can start up from the CD-ROM drive. See [“Using the CD as an Emergency Disk”](#) on page 9.

Once you have created the Emergency Disks, use them to solve the problem.

To use Emergency Disks:

- 1 Turn off your computer using the power switch.
- 2 Insert the Emergency Boot Disk in your A: drive.
- 3 Turn on your computer.

Your computer will start up from the Emergency Boot Disk.

- 4 Press Enter to start the Emergency program.

The Emergency program takes several minutes to load, and then automatically scans your computer and removes viruses.

I cannot start up from my A: drive

There are three likely reasons for this:

- If your computer does not 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 have never used it before, you may want to refer to your computer manufacturer's documentation.

Complete these steps to change the settings:

- a Restart your computer.

A message like this appears telling 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 cannot 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, and then exit the Setup program.

- You need to use a special Boot Disk rather than the Emergency Boot Disk. 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.

Norton AntiVirus Auto-Protect does not 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 option, and then click OK.
- Norton AntiVirus is not configured to start Auto-Protect automatically.
 - a Click the Options button at the top of the Norton AntiVirus main window.
 - b Click Auto-Protect in the list on the left.
 - c Be sure that Start Auto-Protect When Windows Starts Up is checked.

I have scanned and removed a virus, but it keeps infecting my files

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

- The virus might be in a program file with an unusual extension that Norton AntiVirus is not set to look for. Do this:
 - a Click the Options button at the top of the Norton AntiVirus main window.
 - b Click Manual Scans in the list on the left.
 - c Select the All Files option in the What To Scan group.
 - d Expand Manual Scans.
 - e Click Bloodhound.
 - f Set the Heuristics Sensitivity Level to Highest Level Of Protection.
 - g Click OK to save your settings and close the Options dialog box.
 - h 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 to ensure they are free of viruses.
- The virus may remain in memory after you remove it from the boot record. It then reinfects your boot record. Use your Emergency Disks to remove the virus.

Norton AntiVirus cannot repair my infected files

The most common reason that Norton AntiVirus cannot repair your infected files is that you do not have the most current virus protection on your computer. You should update your virus protection regularly to protect your computer from the latest viruses.

- Click the LiveUpdate button at the top of the main window to update your virus protection.

If after using LiveUpdate the virus still can not be repaired, the file may be corrupted, or contain a new virus. There are two additional options:

- Quarantine the file and submit to SARC. See [“Submitting files to SARC”](#) on page 40.
- If a non-infected copy of the file exists, delete the infected file and replace it with the non-infected file.

Some Norton AntiVirus features are password-protected, and I do not know the password

Uninstall Norton AntiVirus, and then reinstall it. This will remove the password.

I can't receive email

If you experience trouble downloading email when Norton AntiVirus email protection is enabled, try the following:

- Temporarily disable email protection. This might allow the problem email to be download so that you can once again enable email protection. You are protected by Auto-Protect while email protection is disabled. See [“To temporarily disable email protection:”](#) on page 47.
- Be sure that POProxy is running. POProxy is the Norton AntiVirus email scanner, and it should start when you start Windows.

To resolve this, make sure that “POProxy” starts with Windows. To determine if POProxy is running, press Ctrl+Alt+Del to display the Windows Task List. Look for a program called POProxy.

If you do not see POPProxy listed, add a shortcut from the \Program Files\Norton AntiVirus\POPProxy.exe file to your computer's Startup folder. For more information about how to create Shortcuts and about your computer's Startup folder, please refer to Windows Help.

- If you continue to experience problems downloading email, disable email protection. See [“To disable email protection:”](#) on page 47.
- Manually reconfigure your email client. If disabling email protection does not solve your problem, you might have to manually reconfigure your email client. In your email client program, change the user name and POP3 server name to the values provided by your ISP. See help for more information.

To temporarily disable email protection:

- 1 At the top of the Norton AntiVirus main window, click Options.
- 2 Click Internet > Email Protection in the list on the left.
- 3 Clear the check mark next to the email client.
- 4 Download your email.
- 5 Reenable email protection.

To disable email protection:

- 1 At the top of the Norton AntiVirus main window, click Options.
- 2 Click Internet > Email Protection in the list on the left.
- 3 Clear the check mark next to the email client.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers several technical support options:

- StandardCare support

Connect to the Symantec Service & Support Web site at <http://service.symantec.com>, then select your product and version. This gives you access to product knowledge bases, interactive troubleshooter, Frequently Asked Questions (FAQ), and more.

- PriorityCare, GoldCare, and PlatinumCare support

Fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

For telephone support information, connect to <http://service.symantec.com>, select your product and version, and then click Go! On the Service & Support page for your product, click Contact Options.

- Automated fax retrieval

Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 984-2490.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for six months after the release of the new version. Technical information may still be available through the Service & Support Web site (<http://service.symantec.com>).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Visit Symantec Customer Service online at <http://service.symantec.com> for assistance with non-technical questions and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at: <http://www.symantec.com/upgrades/> or call the Customer Service Order Desk at (800) 568-9501.

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to <http://www.symantec.com>, select the country you want information about, and click Go!

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

<http://www.symantec.com/>
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

<http://www.service.symantec.com/mx>
+54 (11) 5382-3802
Fax: +54 (11) 5382-3888

Asia/Pacific Rim

Symantec Australia Pty. Ltd.
408 Victoria Road
Gladesville, NSW 2111
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 9850-1000
Fax: +61 (2) 9817-4550

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucris Zaidan, 920
12º andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

<http://www.service.symantec.com/br>
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032
Fax: +353 (1) 811 8033

Automated Fax Retrieval

+31 (71) 408-3782

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

<http://www.service.symantec.com/mx>
+52 (5) 481-2600
Fax: + 52 (5) 481-2626

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

<http://www.service.symantec.com/mx>

Subscription policy

If your Symantec product includes virus, firewall, or web content protection, you might be entitled to receive protection updates via LiveUpdate. The length of the subscription could vary by Symantec product.

When you near the end of your subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your initial subscription ends, you must renew your subscription before you can update your virus, firewall, or web content protection. Without these updates, your vulnerability to attack increases. Renewal subscriptions are available for a nominal charge.

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

April 20, 2001

Norton AntiVirus™

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ☐ CD Replacement

Name

Company Name

Street Address (No P.O. Boxes, Please)

City State Zip/Postal Code

Country* Daytime Phone

Software Purchase Date

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem:

CD Replacement Price	\$ 10.00
Sales Tax (See Table)	
Shipping & Handling	\$ 9.95
TOTAL DUE	

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

☐ Check (Payable to Symantec) Amount Enclosed \$ ☐ Visa ☐ Mastercard ☐ American Express

Credit Card Number Expires

Name on Card (please print) Signature

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234

Please allow 2-3 weeks for delivery within the U.S.

Symantec and Norton AntiVirus are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 2001 Symantec Corporation. All rights reserved. Printed in the U.S.A.





Potential Virus Submission Procedure

Note: Only use this form if you can't use Scan and Deliver. Scan and Deliver sends quarantined virus samples to the Symantec AntiVirus Research Center via the Internet. See "To submit a quarantined file to SARC" in online help.

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 (ver. _____) ☐ Windows 95/98 ☐ Windows NT/Windows 2000 ☐ 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: You can Quarantine a suspicious file and send it to SARC via the Internet for analysis using Scan and Deliver. For more information, see “To submit a quarantined file to SARC” in online help.

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.
- 2 Press function key F8 before Windows starts and choose “Safe mode command prompt only” from the on-screen menu.
- 3 Format a floppy disk with the potentially infected operating system.
From the DOS prompt, type `FORMAT A: /S` and press Enter.
- 4 Copy `MODE.COM`, `MEM.EXE`, `KEYB.COM`, and `XCOPY.EXE` from your `C:\WINDOWS\COMMAND` folder to the floppy disk.
- 5 Type `A:` and press Enter to change to the A: drive.
- 6 Type `PATH;` and press Enter (don’t forget the semicolon) to remove the path from the environment temporarily.
- 7 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.
- 8 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.
- 9 Label the floppy disk with your name, address, telephone number, and the date of its creation. Write “Potential Virus” on the disk label.
- 10 Complete and send the form on the previous page with the floppy disk to Symantec.

I N D E X

A

- ActiveX controls 14
- alert actions 35
- alerts
 - actions to take 35
 - Norton AntiVirus 23-25
 - virus found 23-25, 36
 - virus-like activity 37-38
- AOL 19
- applications
 - avoiding infected 30
 - backup copies 30
 - disabling virus protection when installing 31
 - virus-like activity 37-38
- attachments, email 14, 28
- Automatic LiveUpdate 10, 13
- Auto-Protect
 - enabling 32, 45
 - failure to load on startup 45
 - icon 29, 31
 - maintaining protection 30-31
- avoiding viruses 27

B

- backup copies
 - infected 36, 39
 - replacing infected files 39
 - software 30
- boot records, unable to repair 39
- booting
 - Auto-Protect failure to load 45
 - changing floppy drive settings 44
 - floppy drive fails 44

C

- compressed files 14, 29

D

- deleting infected files 36, 39
- disabling Auto-Protect 31
- downloads, scanning automatically 29
- drives, scanning 32

E

- email protection 13, 14, 28
- Emergency Disks 7, 8
- Emergency Disks, using 9
- emergency procedures 8
- enabling virus protection 29, 30-31, 32, 45
- excluding files from scans 36

F

- file extensions
 - infected files 38
 - scans missing unusual 45
- files
 - reinfected after virus removal 45
 - scanning all 45
- floppy disks, scanning 32
- floppy drives, unable to boot from 44

H

- help 10, 19-21

I

- icon, Auto-Protect 29, 31
- infected files
 - deleting 36
 - excluding from scans 36
 - file extensions 38
 - ignoring 36
 - quarantining 35
 - reinfected 45

infected files (*continued*)
 repairing 35
 unable to repair 38-40, 46
installing
 Norton AntiVirus 7-10
 programs, disabling Auto-Protect 31
Internet, virus protection 29
irreparable system files 40

J

Java applets 14

L

LiveUpdate 11, 15, 18
 automatic 10, 13

M

malicious code 14
master boot record 39
memory, removing viruses from 37

N

Norton AntiVirus
 alerts 23-25
 basics 17-21
 emergency procedures 35-41
 features 14-15, 28
 installing 7-10
 procedures 27-32

O

online help 10, 19-21
options, setting 18

P

password 46
preventing viruses 27
programs
 avoiding infected 30
 backup copies 30

programs (*continued*)
 disabling virus protection when
 installing 31
 virus-like activity 37-38
protection. *See* virus protection

Q

Quarantine 14, 35, 40

R

removing
 infected files 39
 viruses during installation 8
 viruses from memory 37
repairing
 infected files 35
 unsuccessful 38-40, 46
requirements, system 7

S

safe mode 45
SARC 40
Scan and Deliver 40
scanning
 all files 45
 compressed files 29
 drives 32
 email 14, 28
 floppy disks 32
Service and Support 49
setup program, changing boot drive
 sequence 44
setup, Norton AntiVirus 7-10
Smart Scanning Technology 13
SmartScan 13
software
 avoiding infected 30
 backup copies 30
 disabling virus protection when
 installing 31
 virus-like activity 37-38

startup

- Auto-Protect failure to load 45
- changing floppy drive settings 44
- floppy drive fails 44
- subscription, virus protection 18
- system files, unable to repair 40, 46
- system requirements 7

T

- Technical Support 49
- Trojan Horses 14, 28
- troubleshooting 43-46

U

- uninstalling 11
- updating virus protection 11, 15, 18, 29

V

virus

- removal tools 39
- submitting to SARC 40
- virus alerts. *See* alerts
- virus protection
 - compressed files 29
 - downloads 29
 - email 28
 - enabling 29, 45
 - maintaining 10
 - Norton AntiVirus features 28
 - subscription 18
 - updating 15, 29
 - user responsibilities 29
 - virus protection 29

viruses

- alerts 23-25
- avoiding 27, 29-30
- behavior 27
- new 29
- protection from 14
- removing during installation 8
- understanding 27
- virus-like activity alerts 37-38

W

- What's This? help 20
- Windows safe mode 45
- worm 28