

# Norton AntiVirus™ User's Guide

**NORTON**

**AntiVirus™** 2000 VERSION 6.0

# 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 © 1995-1999 Symantec Corporation. All Rights Reserved.

Norton AntiVirus2000

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, 10201 Torre Avenue, Cupertino, CA 95014.

## Trademarks

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

Windows is a registered trademark of Microsoft Corporation. Iomega is a registered trademark and Zip, Zip Rescue are trademarks of Iomega 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 ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THESE TERMS CAREFULLY. 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 only one copy of one version of the various versions of the Software contained on the enclosed media on a single computer, or if only one version is contained on the enclosed media use one copy of such version 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) the primary user of the computer on which the Software is installed may also use the Software on a single home computer if he or she returns the completed product registration card which accompanies the Software.

### YOU MAY NOT:

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

### SIXTY DAY MONEY BACK GUARANTEE:

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

### LIMITED WARRANTY:

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

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

### DISCLAIMER OF DAMAGES:

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

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

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. THE DISCLAIMERS AND LIMITATIONS SET FORTH ABOVE WILL APPLY REGARDLESS OF WHETHER YOU ACCEPT THE SOFTWARE.

### U.S. GOVERNMENT RESTRICTED RIGHTS:

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

### GENERAL:

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



# Welcome to Norton AntiVirus

Dear Norton AntiVirus 2000 Owner,

Congratulations on selecting the #1 antivirus software! You've joined millions of satisfied Norton AntiVirus customers protecting their computers automatically from viruses and other threats. We appreciate your confidence in Symantec and thank you for choosing Norton AntiVirus 2000!

Computer viruses are a growing problem. Ten to 15 new viruses are created each day. By using Norton AntiVirus 2000, you are protecting your valuable computer with the strongest possible antivirus technology against viruses, Trojan horses, ActiveX controls, and Java applets. Now you can feel confident receiving email, downloading files from the Internet, working on a network, or opening files from a floppy disk.

Email is now the most common way for people to receive viruses and other malicious code. Prevention is easy but important. Select the new email scanning feature during install to automatically configure Norton AntiVirus 2000 to check incoming email and attachments for viruses. Also, set the LiveUpdate feature to automatically update the virus definitions using the Internet. Unique to Norton AntiVirus, these updates are downloaded and installed automatically and in the background with no need to reboot your computer! Be sure to update your virus definitions at least every two weeks.

Norton AntiVirus 2000 includes these new features: Automatic Email Scanning, Windows-based Virus Alerts, Better Compressed File Support, Internet Messaging with LiveAdvisor, Searchable Virus List, Virus Definition Alerts.

You can get special assistance for any new threat easily and quickly with Scan and Deliver. This unique feature allows you to get help with new virus problems directly from our researchers at the Symantec AntiVirus Research Center who can then speed solutions to you before most companies have even heard of them!

If you haven't yet installed Norton AntiVirus 2000, please begin by reading the "Installing Norton AntiVirus" chapter in this user's guide.

Thank you for selecting Norton AntiVirus 2000.

Sincerely,

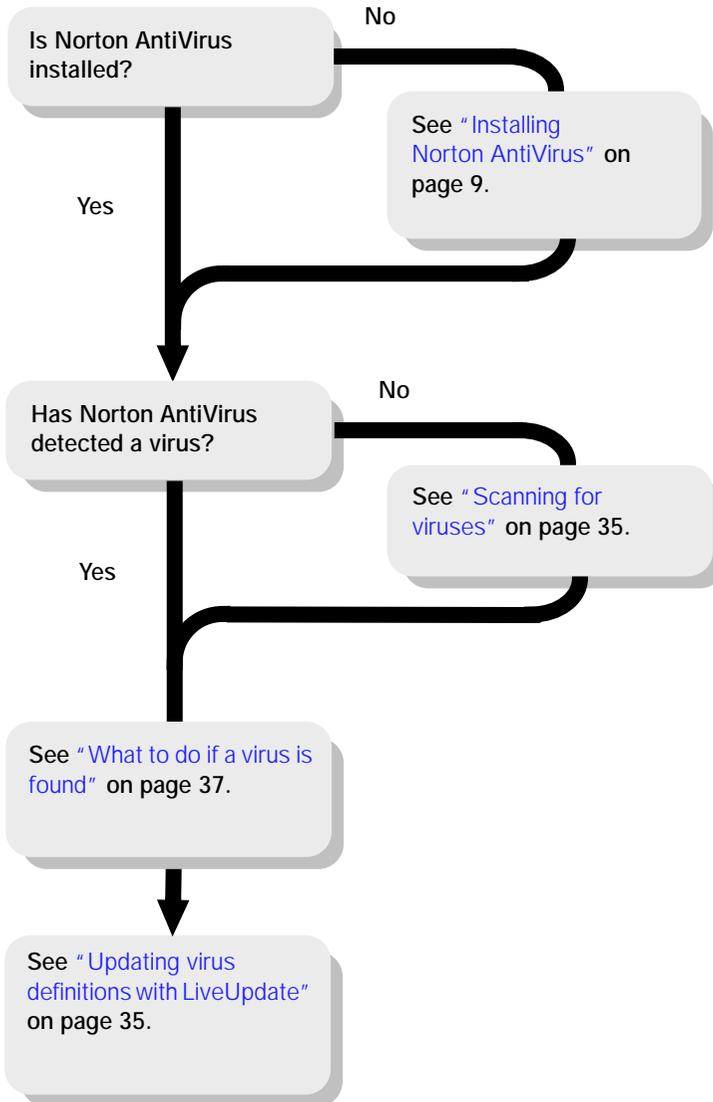
A handwritten signature in black ink, appearing to read "J.W. Thompson", with a long horizontal flourish extending to the right.

John W. Thompson

Chairman, President and Chief Executive Officer

Symantec Corporation

# Help! I've got a virus.



# C O N T E N T S

## Chapter 1 Installing Norton AntiVirus

Installing Norton AntiVirus .....	9
System requirements .....	9
Installation procedure .....	10
Removing viruses when you install .....	10
Keeping your system protected .....	11
LiveUpdate .....	11
LiveAdvisor .....	11
Rescue Disks .....	11
Uninstalling Norton AntiVirus .....	12

## Chapter 2 Introducing Norton AntiVirus

What's new in Norton AntiVirus 2000 .....	13
Norton AntiVirus .....	13

## Chapter 3 Norton AntiVirus basics

Navigating Norton AntiVirus .....	17
Setting options .....	18
Updating Norton AntiVirus with LiveUpdate .....	18
Using LiveAdvisor .....	19
Creating Rescue Disks .....	19
Creating Norton Zip Rescue Disks .....	20
Creating basic Rescue Disks .....	22
Updating Rescue Disks .....	23
Using help to learn more about Norton AntiVirus .....	25

## Chapter 4 Responding to Norton AntiVirus alerts

Norton AntiVirus alerts .....	27
-------------------------------	----

## Chapter 5 Preventing viruses with Norton AntiVirus

Understanding and avoiding viruses .....	31
Understanding Trojan Horses .....	32
What Norton AntiVirus does automatically .....	32
What you have to do .....	33
Tips for avoiding viruses .....	33
Maintaining full-time protection with Auto-Protect .....	33

---

Turning Norton AntiVirus Auto-Protect off temporarily .....	34
Updating virus definitions with LiveUpdate .....	35
Scanning for viruses .....	35

## Chapter 6 Norton AntiVirus emergency procedures

What to do if a virus is found .....	37
Quick guide to alert actions .....	37
Types of virus alerts .....	38
What to do if Norton AntiVirus cannot repair .....	40
Using Rescue Disks in virus emergencies .....	41

## Chapter 7 Troubleshooting

Requirements for installing .....	49
Installing Norton AntiVirus Windows 3.x/DOS .....	50
Removing viruses when you install .....	50
Turning Norton AntiVirus Auto-Protect off temporarily .....	51
Scan for viruses .....	51
What to do if a virus is found .....	53
Quick guide to alert actions .....	53
Types of virus alerts .....	55
VIRUS FOUND .....	55
VIRUS IN MEMORY .....	55
UNINOCULATED ITEM .....	56
INOCULATION CHANGE .....	56
VIRUS-LIKE ACTIVITY .....	56

## Symantec 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 Rescue Disks (or a Zip™ disk and a floppy disk to make a Norton Zip Rescue™ disk set).

---

**Note:** You do not need to uninstall previous versions of Norton AntiVirus from your system before running Setup.

---

### System requirements

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

- Windows® 95, Windows 98, Windows NT, or Windows 2000
- 486-66 processor, Pentium® recommended
- 16 MB of memory (32 MB for Windows 2000), additional memory recommended
- 45 MB hard drive space (50 MB for Windows NT and Windows 2000)
- CD-ROM drive
- 256-color VGA or better video
- Iomega® Zip or Jaz drive optional

---

**Tip:** While not required, an Iomega Zip drive is a definite advantage when making a Rescue Disk set.

---

---

**Note:** Norton AntiVirus does not support Iomega Zip or Jaz drives with a USB interface because there are no DOS drivers available.

---

## Installation procedure

To install:

- 1 Start Windows (if it is not already running).
- 2 Insert the Norton AntiVirus CD in the CD-ROM drive. An opening screen appears.
- 3 Click Install Norton AntiVirus and follow the on-screen instructions.

---

**Tip:** 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.

The last step of installation is for you to create Rescue Disks. Rescue Disks are an important part of your protection. For example, they let you safely restart your computer if it is halted due to a virus in memory. See [“Creating Rescue Disks”](#) on page 19.

---

**Tip:** While this user’s guide contains helpful information, there is additional information in online help that is not covered here.

---

## Removing viruses when you install

When you install Norton AntiVirus, it scans for viruses in memory. If it finds an active virus, use the Emergency Boot Disk that comes with the product to remove the virus before you can finish installing.

To remove a virus:

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

---

**Note:** If you cannot start up from the A: drive, see [“I cannot start up from my A: drive”](#) on page 46.

---

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

## Keeping your system protected

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

### 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 month.

### LiveAdvisor

LiveAdvisor acts as your personal agent, checking with Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register. See [“Using LiveAdvisor”](#) on page 19.

### Rescue Disks

Rescue Disks contain critical information your computer needs to start and run properly. This information changes as you change the configuration of your computer, so it is important to keep your Rescue Disk set up-to-date.

You should update your Rescue Disks at least once a month, plus any time you update your virus protection, install new software, or make changes to your hardware. See [“Creating Rescue Disks”](#) on page 19.

## 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.

---

**Tip:** You may also want to uninstall LiveAdvisor and LiveUpdate 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 2000

### Email scanning

Norton AntiVirus now scans email attachments as you receive them from the Internet. It integrates with most POP3 clients, which include the most popular Internet mail clients including Outlook Express and Eudora.

### Improved compressed file scanning

Norton AntiVirus can now find and fix viruses and other malicious code inside compressed files, such as zipped files. It can even fix problems in a compressed file that is itself contained in another compressed file. Norton AntiVirus now supports more kinds of compressed files, including ZIP, LHA, CAB, and many more.

## 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.

## Rescue Disk

Rescue Disks keep you prepared to deal with a virus emergencies that can occur without warning. Rescue Disk records a duplicate set of system startup files, CMOS data, and disk partition information, and stores rescue items plus Norton AntiVirus on an Iomega Zip disk, across multiple floppy disks, or on a network drive.

A Norton Zip Rescue Disk set consists of one Zip disk and one bootable floppy disk. With this disk set, you can start Windows 95/98 and use Norton AntiVirus to fix virus-related problems.

A basic Rescue Disk set consists of one bootable floppy disk and several additional disks. With this kind of Rescue Disk set, you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.

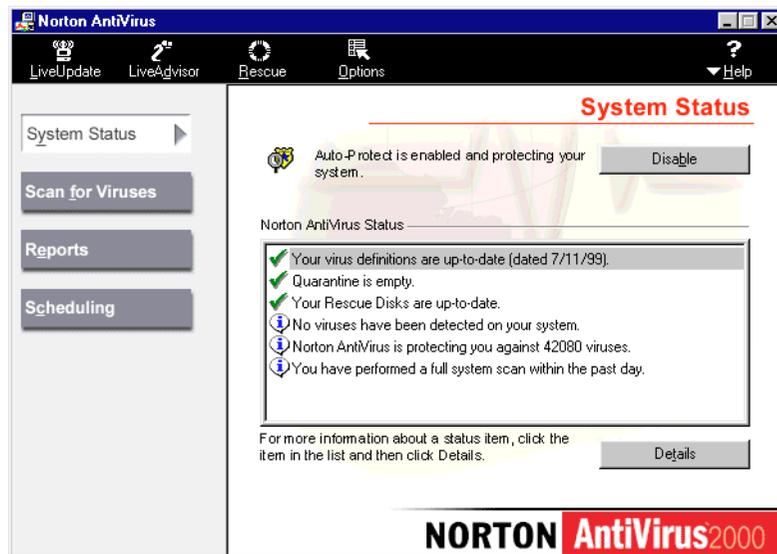


# Norton AntiVirus basics

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

## Navigating Norton AntiVirus

To start Norton AntiVirus, click the Start button, and then select Programs > Norton AntiVirus > Norton AntiVirus or double-click the Norton AntiVirus icon on your desktop.



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

## Setting options

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

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.

---

**Tip:** For maximum protection, always keep the File Types To Scan option set to All Files.

---

## 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 check for updates to your virus protection. LiveUpdate can use a modem or 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:** If you use a modem, toll charges may apply. If you connect through the Internet, 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 LiveAdvisor

If you register over the Internet, you can sign up for LiveAdvisor, a special two-way communication system. LiveAdvisor acts as your personal agent, checking with Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register. For assistance setting up LiveAdvisor, open LiveAdvisor and choose Contents from the Help menu.

If you do not sign up for LiveAdvisor when you register your Symantec product over the Internet, you can do so at any time.

### To start using LiveAdvisor:

- 1 Click the LiveAdvisor button at the top of the Norton AntiVirus main window.
- 2 If the product for which you want LiveAdvisor services is not registered, do this:
  - a Click Profile and select the Products tab.
  - b Select the product and click Register.

## Creating Rescue Disks

Rescue Disks contain critical information your computer needs to start and run properly. This information changes as you change the configuration of your computer, so it is important to keep your Rescue Disks up-to-date.

---

**Note:** If you use Windows NT or Windows 2000 you won't have the option to make Rescue Disks. Windows NT and Windows 2000 provide built-in protection against the problems that require Rescue Disks, so they are not necessary.

---

If you have an Iomega Zip drive, Rescue Disk can use it to make Rescue Disks that let you start Windows 95/98 even when your computer will not start up normally after a system crash. This lets you make emergency repairs.

You can also make Rescue Disks using your standard floppy drive and several floppy disks. This floppy-based set lets you start up to the DOS operating system only, and access DOS-based utilities. Both kinds of Rescue Disks provide you with an easy-to-use interface for recovering from a system crash.

---

**Caution:** Never use Rescue Disks made on another computer. Rescue Disks contain information specific to the computer on which they were made.

---

---

**Tip:** The more recent your Rescue Disks, the better your chances of a full recovery. Update your Rescue Disks whenever you update your virus protection, install new software, or make changes to your hardware.

---

## Creating Norton Zip Rescue Disks

A Norton Zip Rescue Disk set consists of two disks:

- Bootable floppy disk
- Zip disk

You need both of these disks to successfully restore your system after a crash. The floppy disk contains the DOS system files necessary to start up your computer. The Zip disk contains the Windows 95/98 operating system, as well as the startup files, configuration information, and Norton AntiVirus programs necessary to restore your computer.

---

**Note:** Some computer manufacturers replace the standard floppy disk drive with a Zip drive. In this case, your Rescue Disk set will not include a bootable floppy disk. Rescue Disk creates a bootable Zip disk that contains all required Rescue Disk information.

---

---

**Tip:** Rescue disks contain system settings and rescue files. They do not back up your data. Be sure to make adequate backups of all your data.

---

To create a Norton Zip Rescue Disk set:

- 1 Click the Rescue button at the top of the Norton AntiVirus main window.
- 2 Insert a Zip disk in your Zip drive and a floppy disk in your A: drive.

---

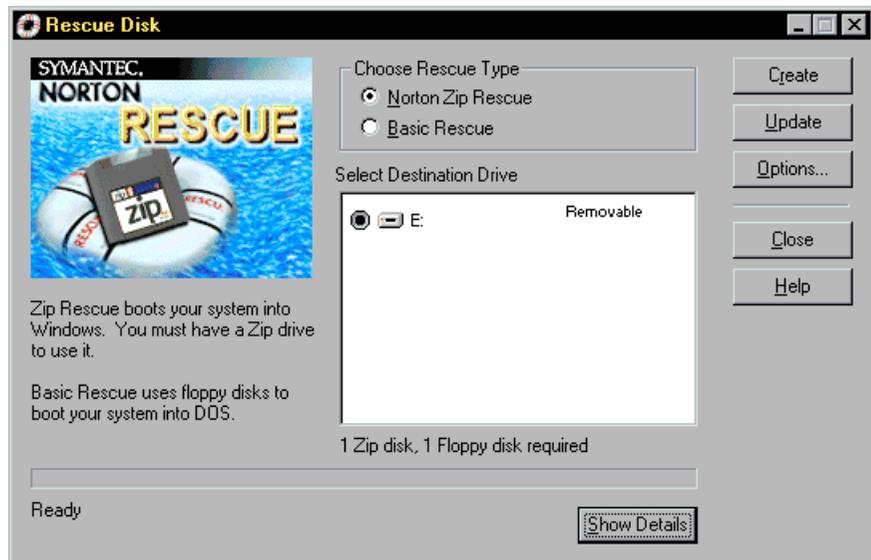
**Note:** Do not use disks that contain data that you want to save. Rescue Disk overwrites all information on the disks.

---

**Tip:** You can also use an Iomega Jaz drive when making this kind of Rescue Disk.

---

- 3 Select Norton Zip Rescue in the Choose Rescue Type group box.



---

**Caution:** If you have multiple Zip drives installed on one computer, make sure to always use the same Zip drive when creating, updating, and using your Norton Zip Rescue Disks.

---

- 4 Click Create.  
Rescue Disk formats both the floppy and Zip disks and copies your computer's essential startup information to the disks.
- 5 Click Restart to test your newly created Rescue Disks.

- 6 If the Rescue Disk window appears on the screen, the Rescue Disk works properly. If the Rescue Disk window does not appear, the Rescue Disk does not work properly.

---

**Caution:** Do not continue with the rescue process when you are testing Rescue Disks. “Repairing” a system that is functioning properly can cause problems.

---

**Note:** If your Rescue Disk does not work, see [“My Rescue Disk does not work”](#) on page 45.

---

- 7 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.
- 8 Shut down Windows if it is running. Turn the power off and on again to restart your computer.

## Creating basic Rescue Disks

Basic Rescue Disks give protection that is indispensable in protecting your computer from disasters. Basic Rescue Disks let you start up your computer to DOS after a system crash and use the DOS-based utilities to fix many problems.

You save your Rescue Disk set to a series of 1.4 MB floppies or a hard drive to which you have access.

To create basic Rescue Disks:

- 1 Click the Rescue button at the top of the Norton AntiVirus main window.
- 2 Select Basic Rescue in the Choose Rescue Type group box.
- 3 Select the drive you want Rescue Disk to use to create the Rescue Disk set. To create a floppy-based disk set select your A: drive.

---

**Caution:** If you select a network drive, a second physical hard disk, or some other large capacity disk drive, your Rescue Disk set is placed in a folder on the selected disk. Make sure to make a bootable floppy or Zip disk and keep it in a safe location. This disk should contain the network drivers or other files necessary to start your computer and access the drive on which you placed your Rescue Disk set. Do *not* create your Rescue Disk set on your C: drive.

---

- 4 Insert a floppy disk into your A: drive.
- 5 Click Create.  
Rescue Disk formats the disk and copies your computer's essential startup information to the disk.
- 6 Insert additional disks as required. Label the disks as you insert them.
- 7 Click Restart to test your newly created Rescue Disks. .
- 8 If the Rescue Disk screen appears on the screen, the Rescue Disk works properly. If the Rescue Disk screen does not appear, the Rescue Disk does not work properly.

---

**Caution:** Do not continue with the rescue process when you are testing Rescue Disks. "Repairing" a system that is functioning properly can cause problems.

---

**Note:** If your Rescue Disk does not work, see ["My Rescue Disk does not work"](#) on page 45.

---

- 9 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.
- 10 Shut down Windows if it is running. Turn the power off and on again to restart your computer.

## Updating Rescue Disks

Because your Rescue Disks contain information about your computer that can change, it is vital that you keep your Rescue Disks current.

You can update your Rescue Disks as often as you like. Rescue Disk lets you quickly and easily update Zip and basic Rescue Disks without having to recreate them.

---

**Caution:** The update feature can track one set of each type of Rescue Disk. If for some reason you choose to keep more than one basic Rescue Disk set or more than one Norton Zip Rescue Disk set, do not use this feature.

---

To update your Rescue Disks:

- 1 Click the Rescue button at the top of the Norton AntiVirus main window.
- 2 Select the type of Rescue Disk set you are updating in the Choose Rescue Type group box.
- 3 Specify the location of your Rescue Disks:
  - For Norton Zip Rescue Disks, insert the Zip disk into your Zip drive and the floppy disk into your floppy drive.
  - For basic Rescue Disks, select the drive in the Select Destination Drive list box. If you are updating floppy-based Rescue Disks, insert the first disk of the set into your A: drive.

---

**Caution:** If you have multiple Zip drives installed on one computer, make sure to always use the same Zip drive when creating, updating, and using your Norton Zip Rescue Disks.

---

- 4 Click Update.  
Rescue Disk updates your computer's essential startup information on the disks.
- 5 Click OK to test the newly updated Rescue Disks.
- 6 If the Rescue Disk screen appears on the screen, the Rescue Disk works properly. If the Rescue Disk screen does not appear, the Rescue Disk does not work properly.

---

**Caution:** Do not continue with the rescue process when you are testing Rescue Disks. "Repairing" a system that is functioning properly can cause problems.

---

---

**Note:** If your Rescue Disk does not work, see ["My Rescue Disk does not work"](#) on page 45.

---

- 7 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.
- 8 Shut down Windows if it is running. Turn the power off and on again to restart your computer.

# 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.

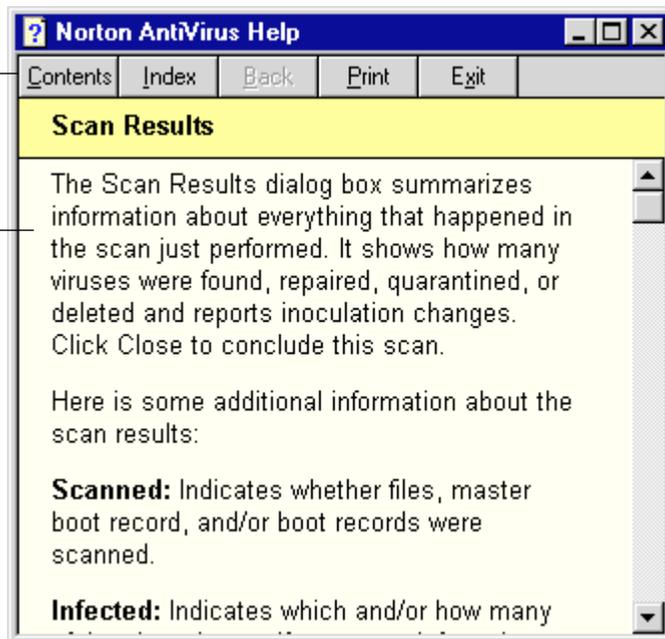
To get help with a dialog box:

- Click the Help button located in the dialog box.

A help topic pertaining to the current dialog box appears.

Complete table of contents and index

Information about the dialog box and how to use it



## 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.

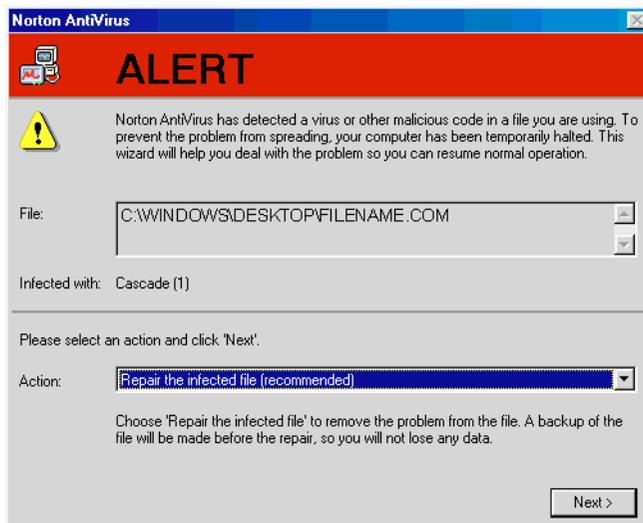
## Norton AntiVirus alerts

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.

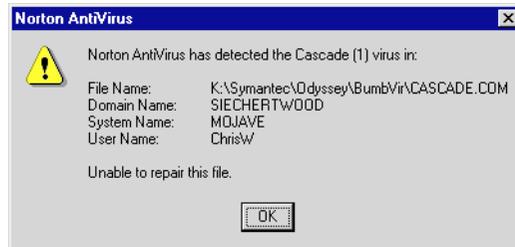
If you see this type of alert:



- 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 . 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 35.

---

**Note:** Norton AntiVirus is preset to deny access to infected files on Windows NT and Windows 2000. You can configure Auto-Protect to automatically repair infected files, or to take other actions. See online help for more information.

---



# 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.

## 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.

## 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. You can do this with LiveUpdate or by mail. To update virus protection, see [“Updating virus definitions with LiveUpdate”](#) on page 35.
- Update your Norton Rescue Disks each time you update your virus protection or make changes to your computer’s hardware or operating system (for example, when you add a disk drive). To update Rescue Disks, see [“Updating Rescue Disks”](#) on page 23.

## 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 update your virus protection from Symantec to keep up with the new viruses that have been released since you installed 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 [“Scanning for viruses”](#) on page 35.

## 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:

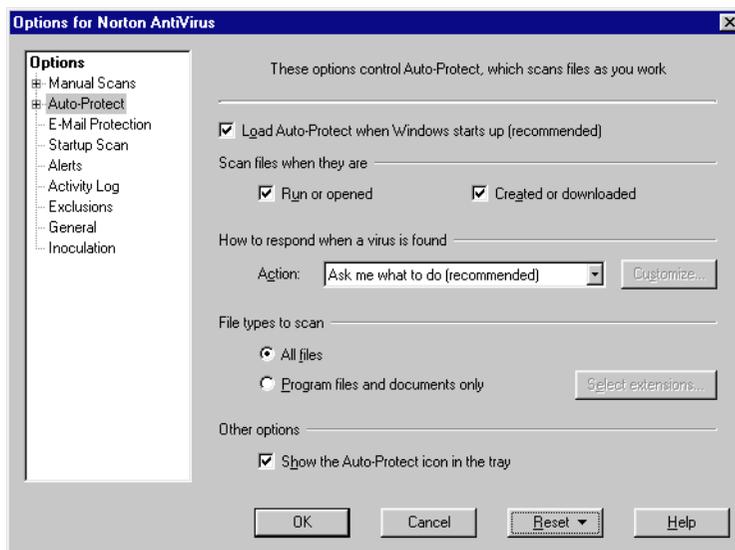
- 1 Start Norton AntiVirus.
- 2 Check that it says “Auto-Protect is enabled.” If it says “Auto-Protect is disabled,” click the Enable button.

- 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 Load Auto-Protect When Windows Starts Up is checked.

---

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

---



## Turning Norton AntiVirus Auto-Protect off temporarily

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

You are sometimes told to disable your 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.

## Updating virus definitions with LiveUpdate

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

## 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.

---

**Note:** If what you want to scan is not in the list, click Create New Scan to start the Scan Wizard, which will help you build a custom scan.

---

- 4 Click Run Scan Now.

---

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

---



# Norton AntiVirus emergency procedures

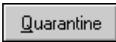
## What to do if a virus is found

When you see one of the Norton AntiVirus alerts shown in [“Responding to Norton AntiVirus alerts”](#) on page 27, you can use the information in this chapter to help you respond appropriately.

### 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.

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 40.

### 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 write-protected Rescue 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 Rescue Boot Disk into the A: drive.
- 3 After waiting a few seconds, turn the computer on.  
If you do not have Rescue Disks, see [“The alert tells me to use my Rescue Disks, but I did not create them”](#) on page 46.
- 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 46.

## 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 virus definitions with LiveUpdate”](#) on page 35.
- 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 filenames that include .COM or .EXE. Document files such as .DOC, .DOT, and .XLS can also 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 Rescue 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.

If Norton AntiVirus cannot repair a file:

Do one of the following:

- Select Quarantine.  
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, 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 cannot repair your hard drive or master boot record, you can use your up-to-date Rescue Disks to restore it. For details, see [“Using Rescue Disks in virus emergencies”](#) on page 41.

If your Rescue Disks are not up-to-date, contact Symantec Technical Support. See the Service and Support Solutions in this guide for contact information.

## 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 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

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 drive. Often, a Norton AntiVirus alert will tell you when to use your Rescue Disks.

You first need to determine whether your Rescue Disks are current. This means that you have created or updated your Rescue Disks since you last did any of the following:

- Added, modified, or removed internal hardware

- Added, modified, or removed hard drive partitions (with software such as Partition-It or Partition Magic)
- Upgraded your operating system (to Windows 98, for example)

---

**Caution:** If the critical information stored on the 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 current Rescue Disks, the following procedure is safe to attempt.

---

---

**Note:** It's OK if you have updated your virus protection since you last updated your Rescue Disks. They may not be able to recognize every new virus, but they will not harm your system simply because the virus protection is out-of-date.

---

---

**Tip:** If your Rescue Disks are not current (see the Caution above) you can still use them to remove viruses from your computer. When the Rescue Disk screen starts from the Rescue Boot disks, use only the Norton AntiVirus task.

---

#### To use your Rescue 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 write-protected Rescue 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.

---

**Tip:** If your Rescue Disks are not current (see the Caution above) you can still use them to remove viruses from your computer. When Norton Rescue starts from the Rescue Boot disks, use only the Norton AntiVirus task.

---

You are prompted when it is time to insert other Rescue Disks.

- 5 When the process is complete, remove the Rescue Disk from the A: drive and restart your computer.

---

**Note:** Virus emergencies are handled by the first two tasks in Norton Rescue: Rescue Recovery and Norton AntiVirus. You should not need any additional tasks listed in Norton Rescue to solve virus emergencies.

---



# Troubleshooting

The following procedures cover the most frequent problems that you may experience.

## My Rescue Disk does not work

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

- If you have a special startup disk for your computer, add it to your Rescue Disk set. In an emergency, start up 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 Boot Disk. At the DOS prompt, type `A:RSHELL`, press Enter, and then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Rescue Boot Disk bootable. Make sure to test your modified Rescue Boot Disk.
- If you are having trouble with a Norton Zip Rescue Disk set, check the `TROUBLE.TXT` file on the Rescue Boot Disk. At the DOS prompt, type `A:VIEW < TROUBLE.TXT` and then press Enter.

Sometimes, your 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 drive, insert your Rescue Boot Disk into the A: drive, and, from a DOS prompt, type `SYS A:` and press Enter. This transfers the operating system to the Rescue Boot Disk. Be sure to retest your Rescue Disks.

---

**Tip:** See “[Creating Rescue Disks](#)” on page 19.

---

### The alert tells me to use my Rescue Disks, but I did not create them

This software package includes a floppy disk called an Emergency Boot Disk. Although it is not as powerful as the Rescue Disks you create, you can use the Emergency Boot Disk to recover from most common emergencies.

- 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 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 setting:

- a Restart your computer.  
A message like this appears telling you the key or keys to press to run SETUP:  

```
Press <DEL> 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 Rescue 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. For more information, see ["My Rescue Disk does not work"](#) on page 45.

## 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.
  - a Choose Norton AntiVirus from the menu.
  - 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 two reasons a virus may continue to infect files:

- The virus may 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 Choose Norton AntiVirus from the menu.
  - c Click Manual Scans in the list on the left.
  - 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 to ensure they are free of viruses.

## **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.

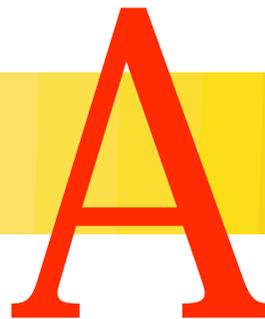
- Click the LiveUpdate button at the top of the main window to update your virus protection.

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 online help to learn how to do this.
- 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.



# Norton AntiVirus for Windows 3.1/DOS

---

**Note:** This abbreviated section will help you get Norton AntiVirus installed under Windows 3.1. You should print the *Norton AntiVirus for Windows 3.1/DOS User's Guide* that is on the Norton AntiVirus CD.

---

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
- Protection when you download files from the Internet

## Requirements for installing

Your computer requirements are:

- 386 IBM or compatible PC with 4 MB of memory
- Microsoft Windows, version 3.1x
- DOS version 5.0 or higher
- 10 MB of free hard disk space to install Norton AntiVirus for Windows and DOS
- 5 MB of free hard disk space to install only Norton AntiVirus for DOS

---

You also must have:

- Two 1.44 MB floppy disks and two disk labels (for Rescue Disks)

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 let you safely restart your computer if it is halted due to a virus in memory.

## Installing Norton AntiVirus Windows 3.x/DOS

For the most complete protection, press Enter to accept all preset options.

To install:

- 1 Do one of the following:
  - Insert the CD into the CD-ROM drive.
  - Insert Norton AntiVirus Installation Disk 1 in the A: drive.
- 2 From the Program Manager File menu, choose Run.
- 3 Click the Browse button, and choose the drive for your floppy disk or CD from the Drives list.
- 4 Do one of the following:
  - For a CD, select NAVDOSWN\SETUP.EXE, and then click OK.
  - For floppy disks, select SETUP.EXE, and then click OK.
- 5 Follow the on-screen instructions. The preselected options will provide you with maximum protection.

If Norton AntiVirus can't install because it finds a virus, see "Removing viruses when you install" in this section.
- 6 Test your Norton Rescue Boot Disk.

## Removing viruses when you install

When you install Norton AntiVirus, it scans for viruses. If it finds an active virus, you will have to use the Emergency Boot disk that comes with the product to remove the virus before you can finish installing.

To remove the virus:

- 1 Turn off your computer using the power switch.
- 2 Insert the Emergency Boot Disk that came with Norton AntiVirus in your A: drive.

- 3 Turn on your computer.  
The Norton AntiVirus Emergency Boot Disk dialog box appears.
- 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.

## 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 left corner of the 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 computer programs. In this case, disable Auto-Protect temporarily and then turn it back on again.

**To turn off Norton AntiVirus Auto-Protect temporarily:**

- 1 Double-click the Norton AntiVirus Auto-Protect icon in the lower left corner of the Windows desktop. (You may have to move windows around to find it.)
- 2 Click Disable.

**To turn on Norton AntiVirus Auto-Protect:**

- Click Norton AntiVirus Auto-Protect in the Norton AntiVirus program group box.

## Scan for viruses

You should scan all floppy disks before you use them.

**To scan drives for viruses:**

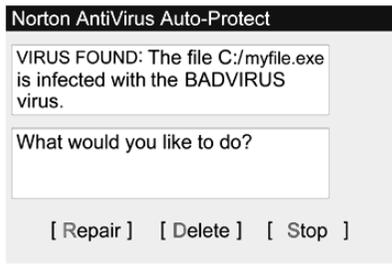
- 1 Double-click Norton AntiVirus in the Norton AntiVirus group box.
- 2 In the Norton AntiVirus main window, do one of the following:
  - Check specific drives in the Drives list box.
  - Select multiple drives in the Drive types box.
- 3 Click Scan Now.

---

To scan individual files or directories for viruses:

- 1 Double-click Norton AntiVirus in the Norton AntiVirus group box.
- 2 From the Scan menu at the top of the Norton AntiVirus main window, choose Directory or File.
- 3 Make your choice and click Scan.

# What to do if a virus is found



If you see a virus alert

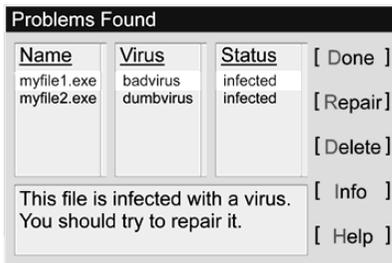
- 1 Look for words that identify the type of problem. Read the whole message.
- 2 Choose the action that is preselected for you or follow the recommendation on the screen.
- 3 If you need more information to decide what to do, find the type of problem in the next few pages.

For example, if the message says VIRUS FOUND, look for “VIRUS FOUND.”



If you see the 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” below 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 press Enter to accept the recommended selection.

---

Actions	When and why you use them
	Eliminates the virus and repairs the infected item automatically. For a VIRUS FOUND, Repair is always the best choice.
	Erases both the virus and the infected file. The virus and file are gone forever. Choose 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'll be alerted again the next time you do the same thing.
	Continues the current operation. Only choose Continue if you are sure a virus is not at work. You'll be alerted again. If you're not sure what to do, it's safer to choose Stop.
	If you choose Exclude and a virus is at work, the virus won't be caught. Exclude should be used only by system administrators for system tuning.
	<p>For an UNINOCULATED ITEM, Inoculate stores information about an item in a special file that is later used to ensure your system stays virus-free. You should choose Inoculate.</p> <p>For an INOCULATION CHANGE, Inoculate updates the stored inoculation data for a boot record or file that has changed since it was last inoculated. Inoculation changes fall into two categories:</p> <ul style="list-style-type: none"><li>■ Expected: If you've just updated a program, the boot records and system files may change. In this case, choose Inoculate.</li><li>■ Unexpected: Changes to boot records and system files are usually caused by viruses. If you have not recently upgraded a program, choose Repair.</li></ul>

---

# 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:

- 1 Click Repair (or type `R` if you can't use your mouse).  
Your file is restored to exactly the way it was before the virus infected it. A backup copy of the infected file has a `.vir` extension.
- 2 Delete the `.vir` file from your floppy disk or hard disk.  
If the repair was successful, the virus is gone and your computer is safe.

## 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.

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.
```

Computer is halted. Restart from your write-protected Rescue 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 Norton AntiVirus Rescue Disk labeled "Norton Rescue Boot Disk" into the drive and turn the computer on using the power switch.
- 3 Once the DOS prompt (for example, `A:\>`) appears, type:  
`NAV /REPAIR` and press Enter.

---

## UNINOCULATED ITEM

The Inoculation feature stores information about files (for example, boot records and system files) that are very important to your computer. Later this information is used to verify these items remain virus-free.

If you see an alert similar to this:

```
UNINOCULATED ITEM: The NEWITEM has not been inoculated.
```

- Click Inoculate to store information about the item (or type **C** if you can't use your mouse).

## INOCULATION CHANGE

If Norton AntiVirus detects any changes made to the stored information it keeps about inoculated files, it alerts you. For example, you may see an alert similar to 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:

- Click Inoculate if the change is expected (or type **C** if you can't use your mouse).

For example, if you just updated a program, the boot records and system files may have changed, so you should inoculate.

- Click Repair if the change is not expected (or type **R** if you can't use your mouse).

For example, if you know no one has recently made changes to your system, like those described above, you should repair the file.

## 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 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:

- Click Continue if the message describes a valid activity for the application you are running (or type **C** if you can't use your mouse).

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.

- Click Stop if the detected activity isn't related to what you are trying to do (or type **S** if you can't use your mouse).

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 disk, the activity is invalid.



# Symantec service and support solutions

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

Technical Support and Customer Service solutions vary by country. If you have questions about the services described below, please refer to the section “Worldwide Service and Support” at the end of this section.

---

**Note:** Symantec’s service and support are subject to Symantec’s prices, terms, and conditions in place at the time the service is used.

---

## Registering your Symantec product

Register your Symantec product online during the installation process, if your software offers this feature. You can also register your Symantec product by completing the registration card included with your package and dropping it in the mail, or by faxing it to (800) 800-1438 or (541) 984-8020.

## Using LiveAdvisor

If you register over the Internet, you can sign up for LiveAdvisor, a special two-way communication system. LiveAdvisor acts as your personal agent, checking with Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register. For assistance setting up LiveAdvisor, open LiveAdvisor and choose Contents from the Help menu.

If you do not sign up for LiveAdvisor when you register your Symantec product over the Internet, you can do so at any time.

### To start using LiveAdvisor:

- 1 Click the LiveAdvisor button at the top of the main window.
- 2 If the product for which you want LiveAdvisor services is not registered, do this:
  - a Click Profile and select the Products tab.
  - b Select the product and click Register.

## Virus Protection Updates Subscription Policy

With the purchase of this product, you receive 12 free months of virus protection updates via LiveUpdate. Renewal subscriptions are available for \$3.95 per year.

After using this product for ten months, you will be prompted to subscribe when you start LiveUpdate. Simply follow the on-screen instructions. After your one-year free subscription ends, you must renew your subscription before you can update your virus protection.

To order a subscription, do one of the following:

- Visit our website at: <http://www.shop.symantec.com>
- In the United States, call Customer Service at (800) 441-7234
- Outside the United States, contact your local Symantec office or representative

## Technical support

Symantec offers an array of technical support options designed for your individual needs to help you get the most out of your software investment.

### World Wide Web

The Symantec World Wide Web site (<http://www.symantec.com/techsupp>) is the doorway to a set of online technical support solutions where you will find the following services:

#### Interactive problem solver

Symantec's online interactive problem solver helps you solve problems and answer questions about many Symantec products.

#### Product knowledgebases

Product knowledgebases enable you to search thousands of documents used by Symantec Support Technicians to answer customer questions.

---

## FAQs

Frequently Asked Questions documents, also known as FAQs, list commonly asked questions and clear answers for specific products.

## Ask a Tech

Ask a Tech discussion groups provide a forum where you can ask questions and receive answers from Symantec online support technicians.

## Chat Now!

Chat Now! For selected products this fee-based service provides customers with the ability to discuss technical issues with a Support Analyst in "realtime" over the Internet, using text, files, and HTML.

## File downloads

Point your Web browser to <http://www.symantec.com/techsupp/files> to search for and download technical notes and software updates. You can also click the LiveUpdate button in programs enabled with this feature to automatically download and install software updates and virus definitions.

## Other technical support options

Other Symantec support options include the following:

---

<b>America Online</b>	Type Keyword: SYMANTEC to access the Symantec forum.
<b>CompuServe</b>	Type GO SYMANTEC to access the Symantec forum.
<b>Symantec BBS</b>	Set your modem to 8 data bits, 1 stop bit, no parity and dial (541) 484-6669.
<b>Automated fax retrieval system</b>	To receive general product information, fact sheets and product upgrade order forms directly to your fax machine, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490.  For technical application notes, please call our Technical Support fax retrieval system at (541) 984-2490 and select option 2.

---

---

StandardCare Support	<p>If you can't access the Internet, take advantage of your 90 days of free telephone technical support (from the date of your first call) at no charge to all registered users of Symantec software.</p> <p>Please see the back of this manual for the support telephone number for your product.</p>
PriorityCare and PlatinumCare Support	<p>Expanded telephone support services are available for a fee to all registered customers. For complete information, please call our automated fax retrieval service, located in the United States, at (800) 554-4403 or (541) 984-2490, and request document 070, or visit <a href="http://www.symantec.com/techsupp/phone/index.html">www.symantec.com/techsupp/phone/index.html</a></p>

---

## 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 previous version for six months after the release of the new version. Technical information may still be available through online support.

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will only be available for discontinued products through online services. See the section "Technical support" for online service options.

## Customer Service

You may contact Customer Service online at <http://www.symantec.com/>

Customer Service can assist you with non-technical questions such as:

- Subscribing to the Symantec Support Solution of your choice.
- Obtaining product literature or trialware.
- Locating resellers and consultants in your area.
- Replacing missing or defective CD-ROM's, disks, manuals, etc.
- Updating your product registration with address or name changes.
- Order, return or rebate status.
- Frequently Asked Questions (FAQ's).
- Posting questions to the Customer Service Newsgroup.

---

## Upgrade Orders

For upgrade orders, please call the Customer Service Order Desk or you may visit the upgrade center online at <http://www.symantec.com/upgrades>

## Data Recovery

Symantec provides data recovery in the United States and Canada for PC hard drives with DOS, Windows 3.x, Windows 95, and Windows 98. If you want highly-trained and dedicated professionals to recover your data, contact the Symantec Data Recovery Team at (541) 984-7910 or get more information from the Symantec website (at <http://www.symantec.com/techsupp/recovery>). Or, call our Fax-on-Demand system at (541) 984-2490 and request document #4132.

## Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office. For general information, please contact the Symantec Service and Support Office for your region.

## Service and Support offices

---

<b>NORTH AMERICA</b>	Symantec Corporation 175 W. Broadway Eugene, OR 97401	1 (800) 441-7234 (USA & Canada) 1 (541) 334-6054 (all other locations) Fax: 1 (541) 984-8020
<b>MEXICO</b>	Symantec Mexico Blvd. Adolfo Ruiz Cortines No. 4642 Piso 14 Col. Jardines del Pedregal México, D.F. C.P. 01900	+52 (5) 481-2600 Fax: +52 (5) 481-2626
<b>ARGENTINA</b>	Symantec Argentina Cerritos 1054 Piso 9 1010 Buenos Aires, Argentina	+54 (11) 4811-7526 Fax: +54 (11) 4811-7495
<b>BRAZIL</b>	Symantec Brazil Av. Juruce, 302 - cj 11 São Paulo - SP 04080 011 Brazil	+55 (11) 5561 0284 Fax: +55 (11) 5530 8869
<b>EUROPE</b>	Symantec Ltd. Schipholweg 103 2316 XC Leiden The Netherlands	+31 (71) 408 3111 Fax: +31 (71) 408 3150  Automated Fax Retrieval: +31 (71) 408 3782
<b>ASIA/PACIFIC RIM</b>	Symantec Australia Pty. Ltd. 408 Victoria Road Gladesville, NSW 2111 Australia	+61 (2) 9850 1050 Fax: +61 (2) 9850 1001  Automated Fax Retrieval: +61 (2) 9817 4550

---

Most International Partners provide Customer Service and Technical Support for Symantec products in your local language. For more information on other Symantec and International Partner locations, please visit our Web site at <http://www.symantec.com/> or call our Technical Support automated fax retrieval service, in the United States at 1 (541) 984-2490, choose Option 2, and request document 1400.

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

7/99

# 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.



# 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.  
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

## A

- ActiveX controls 14
- alert actions 37
- alerts
  - actions to take 37
  - Norton AntiVirus 27-29
  - virus 27-29
  - virus found 38
  - virus-like activity 39
- AOL 18
- applications
  - avoiding infected 33
  - backup copies 33
  - disabling virus protection when installing 34
  - virus-like activity 39
- attachments, email 13, 14, 32
- Auto-Protect
  - enabling 35, 47
  - failure to load on startup 47
  - icon 33, 34
  - maintaining protection 33-34
- avoiding viruses 31

## B

- backup copies
  - infected 38, 40
  - replacing infected files 40
  - software 33
- boot records, unable to repair 41
- booting
  - absent 46
  - Auto-Protect failure to load 47
  - changing floppy drive settings 46
  - floppy drive fails 46
  - Rescue Disk fails 45

## C

- compressed files 13, 14, 32
- customer service 62-64

## D

- deleting infected files 38, 40
- disabling Auto-Protect 34
- downloads, scanning automatically 32
- drives, scanning 35

## E

- email 13, 14, 32
- enabling virus protection 32, 33-34, 35, 47
- excluding files from scans 38

## F

- file extensions
  - infected files 40
  - scans missing unusual 48
- files
  - reinfected after virus removal 48
  - scanning all 48
- floppy disks
  - scanning 35
  - unable to repair boot record 41
- floppy drives, unable to boot from 46

## H

- help 10, 25-26

## I

- icon, Auto-Protect 33, 34
- infected files
  - deleting 38
  - excluding from scans 38
  - file extensions 40

---

infected files (*continued*)

- ignoring 38
- quarantining 37
- reinfected 48
- repairing 37
- unable to repair 40-41, 48

installing

- Norton AntiVirus 9-11
- programs, disabling Auto-Protect 34

Internet

- virus protection 32

Iomega Jaz drive 21

Iomega Zip drive 9, 19

irreparable system files 41

## J

Java applets 14

Jaz drive 9

## L

LiveAdvisor 19

LiveUpdate 11, 14, 18, 35

## M

malicious code 14

master boot record 41

memory, removing viruses from 39

## N

Norton AntiVirus

- alerts 27-29
- basics 17-26
- emergency procedures 37-43
- features 13-14, 32
- installing 9-11
- procedures 31-35

## O

online help 10, 25-26

operating systems, multiple 45

options, setting 18

## P

password 48

preventing viruses 31

programs

- avoiding infected 33
- backup copies 33
- disabling virus protection when installing 34
- virus-like activity 39

protection. *See* virus protection

## Q

Quarantine 14, 37

## R

registering Symantec software 59

removing

- infected files 40
- viruses during installation 10
- viruses from memory 39

repairing

- infected files 37
- unsuccessful 40-41, 48

requirements, system 9

Rescue Disks

- absent 46
- creating 19-23
- failure to start from 45
- importance 11
- updating 23
- when to update 33

## S

safe mode 47

scanning

- all files 48
- compressed files 13, 32
- drives 35
- email 13, 14, 32
- floppy disks 35

setup program, changing boot drive sequence 46

setup, Norton AntiVirus 9-11

---

## software

- avoiding infected 33
- backup copies 33
- disabling virus protection when installing 34
- virus-like activity 39

## startup

- Auto-Protect failure to load 47
- changing floppy drive settings 46
- floppy drive fails 46
- Rescue Disk fails 45
- Rescue Disks absent 46

## subscription

- virus protection 18, 60

## Symantec

- customer service 62-64
- technical support 60-64

system files, unable to repair 41, 48

system requirements 9

## T

technical support 60-64

Trojan Horses 14, 32

troubleshooting 45-48

## U

uninstalling 12

updating virus protection 11, 14, 18, 33, 35

## V

virus alerts. *See* alerts

virus protection

- compressed files 32
- downloads 32
- email 32
- enabling 32, 47
- maintaining 11
- Norton AntiVirus features 32
- subscription 18, 60
- updating 14, 33, 35
- user responsibilities 33
- virus protection 32

## viruses

alerts 27-29

avoiding 31, 33

behavior 31

new 33

protection from 14

removing during installation 10

understanding 31

virus-like activity alerts 39

## W

What's This? help 26

Windows safe mode 47

## Z

Zip drive 9

Zip Rescue Disk  
creating 19-23  
updating 23

