Norton AntiVirus for Windows NT User’s Guide

NORTON

AntiVirus™

VERSION 5.0

Norton AntiVirus for Windows NT 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

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

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

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

Trademarks

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

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

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

NAVNT50USG

SYMANTEC LICENSE AND WARRANTY

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

LICENSE AND WARRANTY

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

You may:

(i) use that number of copies of the appropriate titles of the software as have otherwise been licensed to you by Symantec under a Symantec Volume Incentive or Value License, provided that the number of copies of all such titles in the aggregate will not exceed the total number of copies so indicated on such Volume Incentive or Value license;

(ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;

(iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;

(iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and

(v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

You may not:

(i) copy the printed documentation which accompanies the Software;

(ii) sublicense, rent or lease any portion of the Software;

(iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

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

(v) use the server based software products included with the Software if you have not licensed the Norton AntiVirus Solution for server-based products;

(vi) use the suite based software products included with the Software if you have not licensed the Norton AntiVirus Solution Suite;

(vii) use other than the Macintosh versions of the software if you have only licensed the Macintosh versions of the software; or

(viiii) use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version.

Limited Warranty:

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

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

Disclaimer of Damages:

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

U.S. Government Restricted Rights:

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

General:

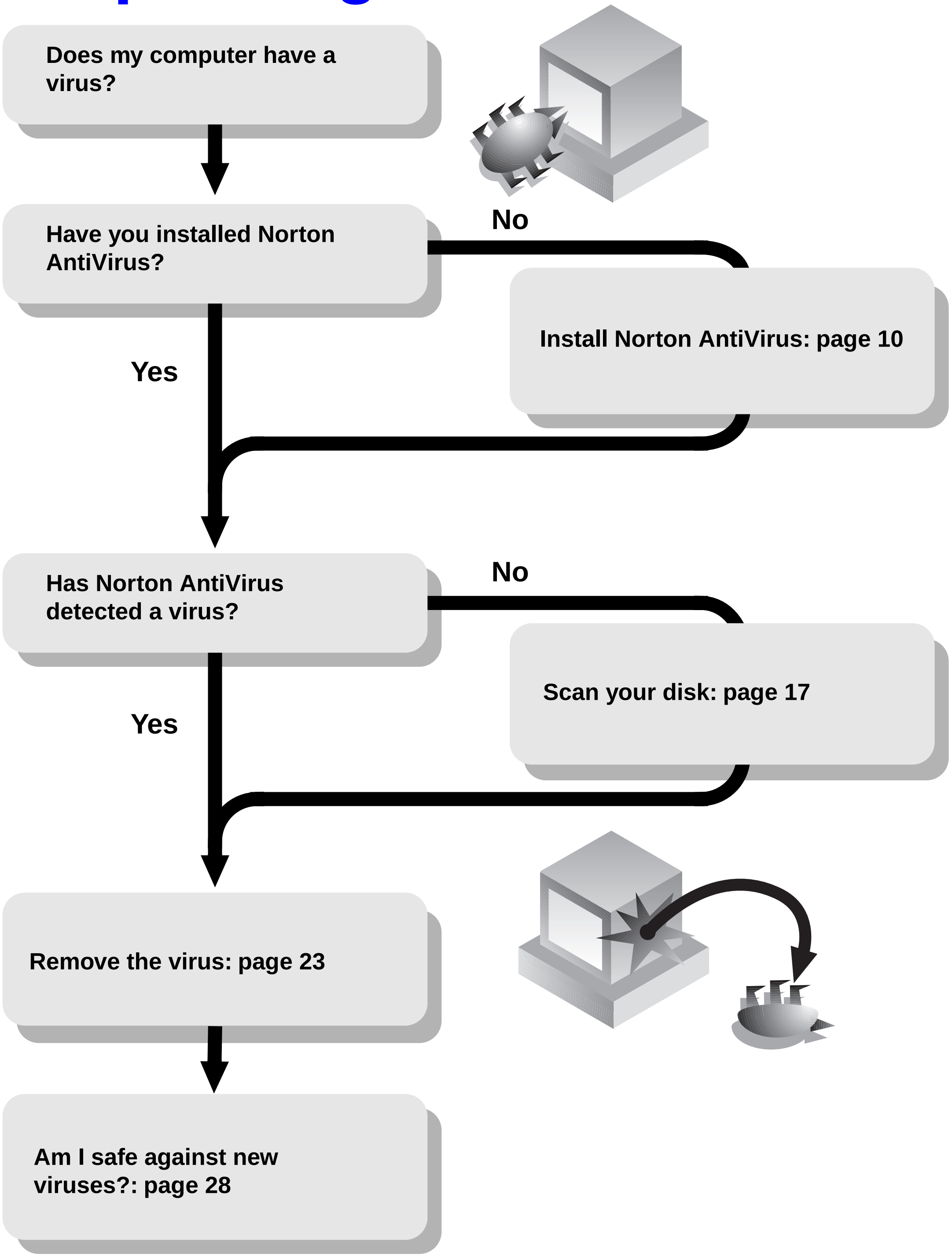
This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you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

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

SYMANTEC SOFTWARE LICENSE ADDENDUM

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

Help! I’ve got a virus!



Does my computer have a virus?

Have you installed Norton AntiVirus?

No

Install Norton AntiVirus: page 10

Yes

Has Norton AntiVirus detected a virus?

No

Scan your disk: page 17

Yes

Remove the virus: page 23

Am I safe against new viruses?: page 28

CONTENTS

Chapter 1 Installation

Chapter 2 Using Norton AntiVirus for Windows NT

Potential Virus Submission Procedure

Index

CHAPTER 1

Installation

Norton AntiVirus for Windows NT

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

- Norton AntiVirus loaded automatically each time you start your computer
- An automatic scan of your disks once per week to ensure they stay virus-free
- Protection when you download files from the Internet

Requirements for installation

You need administrator-level privileges to install Norton AntiVirus for Windows NT. Your minimum computer requirements are:

- 16 MB of memory (32 MB or more recommended)
- Microsoft Windows NT Workstation version 4.0
- 16 MB of RAM (32 MB or higher recommended)
- 24 MB of free hard disk space

Installing Norton AntiVirus for Windows NT

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

To install Norton AntiVirus for Windows NT 4.0:

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

     If the Norton AntiVirus setup program does not start automatically, Autorun may be disabled on your computer.
   - To manually start Norton AntiVirus setup from a CD, insert the Norton AntiVirus CD in your CD-ROM drive, double-click the My Computer icon on the Windows desktop, double-click your CD-ROM drive, then locate and double-click Setup.
   - To install from floppy disks, insert Norton AntiVirus Disk 1 in the A: drive, click Start on the Windows taskbar, click Run, type `A:SETUP` in the text box, then click OK.
2. Follow the on-screen instructions. Questions? See below.

Questions when installing

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

What the choices are	What you should do	Why
Select the folder for Norton AntiVirus.	Accept the preset choice	There's no reason not to. The choice is there for unusual circumstances.
Schedule weekly scans of your local hard disks that run automatically?	Leave this checked.	A weekly scan makes sure your disks stay virus-free.
Automatically start Auto-Protect.	Leave this checked.	Auto-Protect constantly monitors your computer to make sure a virus doesn't infect.
Run LiveUpdate after installation.	Leave this checked if you have a modem or an Internet connection.	LiveUpdate connects to a special Symantec site and updates Norton AntiVirus automatically to protect against newly discovered viruses.
Norton AntiVirus has detected a Netscape browser. Do you want to install plug-ins?	Choose Yes.	This option allows Norton AntiVirus to scan files for viruses when you download using a Netscape browser.
Scan for viruses after installation.	Leave this checked.	Makes sure that your computer is virus-free.

Uninstalling Norton AntiVirus

To uninstall Norton AntiVirus:

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

Using Norton AntiVirus for Windows NT

2

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

What viruses do

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

What viruses don't do

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

What Norton AntiVirus does automatically

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

- Eliminates viruses and repairs files.
- Makes sure your computer is safe from viruses at startup.

- Checks for viruses every time you use software programs on your computer, floppy disks, and document files that you receive or create. (For example, the newest kind of viruses are spread via Microsoft Word and Excel macros.)
- Monitors your computer for any unusual symptoms that may indicate an active virus.
- Runs a scheduled scan automatically once per week to confirm that your hard disks are virus-free.

Internet Protection: As part of regular operation, Norton AntiVirus with its default settings gives 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 and files within compressed files when they are extracted.

What you have to do

To update virus protection, see page 2-28.

Regularly obtain from Symantec updated information that Norton AntiVirus needs to keep your virus protection up-to-date.

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

Tips for avoiding viruses

To avoid computer viruses, follow these rules:

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

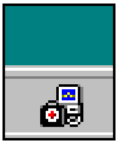
To scan disks, see page 2-17.

- Scan all files on disks you receive from other people.

Turning Norton AntiVirus Auto-Protect off temporarily

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

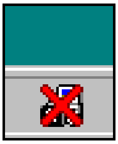
WHY? You are sometimes told to disable your antivirus software when you are installing new computer programs. In this case, you disable Auto-Protect temporarily and then turn it back on again.



To turn off Norton AntiVirus Auto-Protect temporarily:

Do one of the following:

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



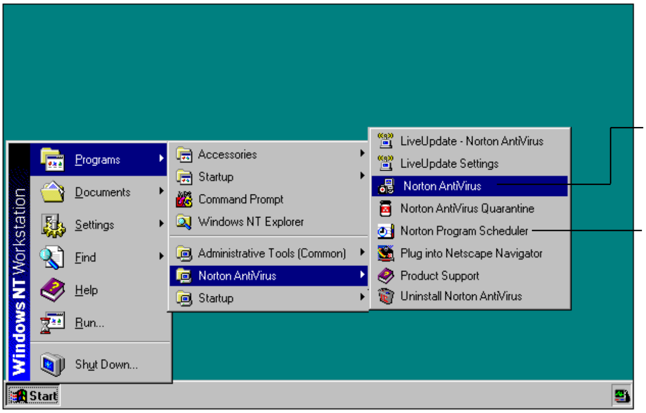
To turn on Norton AntiVirus Auto-Protect:

Do one of the following:

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

What else can I do with Norton AntiVirus?

From the Norton AntiVirus for Windows group on the Start menu, you can access several Norton AntiVirus features.



Start Norton AntiVirus

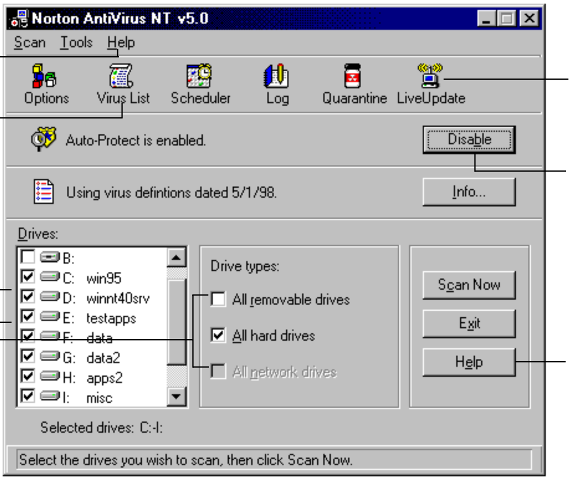
Schedule automatic scans and LiveUpdate

Start Norton AntiVirus

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

To open the Norton AntiVirus window:

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



Auto-Protect is enabled.

Using virus defintions dated 5/1/98.

Drives:

☐ B:
☑ C: win95
☑ D: winnt40srv
☑ E: testapps
☑ F: data
☑ G: data2
☑ H: apps2
☑ I: misc

Drive types:

☐ All removable drives
☑ All hard drives
☐ All network drives

Selected drives: C:-I:

Select the drives you wish to scan, then click Scan Now.

Choose Contents from the Help menu for all topics

Click to view descriptions of known viruses

Select drives to scan for viruses

Click to update your virus protection online

Click to disable or enable Auto-Protect

Click to get a description of everything you can do from this window

Get help

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

To get help using Norton AntiVirus:

Do one of the following:

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

Scan for viruses

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

To scan drives for viruses:

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, do one of the following:
   - Check specific drives in the Drives list box.

- Select multiple drives by checking items in the Drive types box.

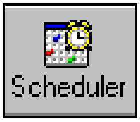
3. Click Scan Now.

To scan individual files or folders for viruses:

1. 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 folder, Path, or File.
3. Make your choice and click Scan.

Tip: To quickly scan a drive, folder, or file, right-click an item in a My Computer or Windows NT Explorer window and choose Norton Virus Check.

Schedule virus scans



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

To schedule a scan:

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click Scheduler.
3. Click Add.
4. Select Scan For Viruses for the Type Of Event.
5. The `/L` in the What To Scan text box tells Norton AntiVirus to scan all local drives.

   You could also enter specific drive letters (for example, C: D:) instead. For a complete list of options, see “Command-line switches” on page 2-21.
6. Select Weekly for the Frequency.
7. Click OK to close the dialog box, then click OK again to confirm.
8. Click the Exit button in the upper-right corner of the Norton Scheduler dialog box.

   Your computer must be turned on when the scan is due to take place.

Customize Norton AntiVirus

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

To customize Norton AntiVirus protection:

1 Start Norton AntiVirus.

2 Click the Options button in the Norton AntiVirus main window.

3 Click one of the tabs in the Options dialog (for example, Alerts).

The dialog changes to show options for the selected feature.

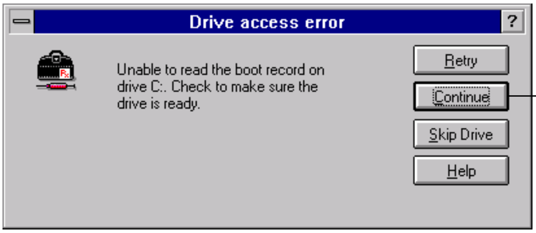
4 Click Help to get information about options.

5 Make your changes and click OK to exit.

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

Bypass boot record scans

WHY? Norton AntiVirus is preset to scan your disk's boot records for viruses as part of its regular operation. As a security precaution, some NT systems are configured to prevent users from accessing these disk areas. You must have administrator-level rights to scan boot records. If you see a dialog box saying that you cannot access the boot records, you can set a configuration option to bypass boot record scans.



Unable to read the boot record on drive C:. Check to make sure the drive is ready.

Click to skip only the boot records and continue the scan

To bypass boot record scans:

1 Start Norton AntiVirus.

2 Click Options in the Norton AntiVirus main window.

3 Click the Scanner tab.

4 Uncheck the first two items in the What to Scan group box:

- Master Boot Record
- Boot Records

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

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

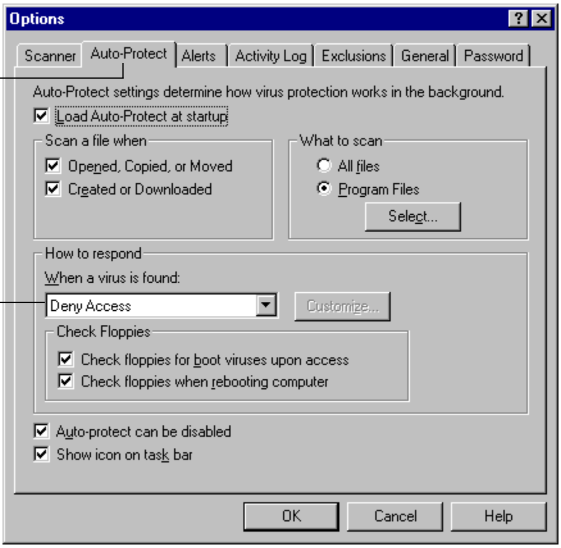
Change how Auto-Protect works

WHY? Norton AntiVirus Auto-Protect, which checks for viruses as you run programs and open documents, is preset to Deny Access to an infected file during regular computer operation. This means that you can't run an infected program or open an infected document. If Auto-Protect detects a virus, you have to start a Norton AntiVirus scan to eliminate the virus. You can change how Auto-Protect works to either repair or delete an infected file automatically.

To change how Auto-Protect works:

1 Start Norton AntiVirus.

2 In the Norton AntiVirus main window, click Options, then click the Auto-Protect tab.



Auto-Protect settings determine how virus protection works in the background.

☑ Load Auto-Protect at startup

Scan a file when

☑ Opened, Copied, or Moved

☑ Created or Downloaded

What to scan

○ All files

● Program Files

How to respond

When a virus is found: Deny Access

Check Floppies

☑ Check floppies for boot viruses upon access

☑ Check floppies when rebooting computer

☑ Auto-protect can be disabled

☑ Show icon on task bar

Click Auto-Protect

Choose how to respond when a virus is detected

3. Click to choose the How To Respond When A Virus Is Found setting:
   - Deny Access: Prevents you from using a file when a known virus is detected. These events are recorded in the Activity Log.
   - Prompt If Logged In: Informs you when a virus is found and lets you choose how to respond. You must be logged in to the computer for this setting. If no one is logged in, Deny Access applies.
   - Repair Automatically: Repairs an infected file or boot record without notifying you. The results of the repair are recorded in the Activity Log. If the file cannot be repaired, access is denied.
   - Delete Automatically: Deletes an infected file without asking you. The file deletion results are recorded in the Activity Log. Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be recovered.
   - Custom Response: Lets you specify different actions for file, macro, and boot virus detections. After selecting Custom Response, click Customize to specify the actions.
   - Quarantine Automatically: Isolates the virus-infected file in a special safe location for later treatment. You can submit the file to the Symantec AntiVirus Research Center (SARC) for analysis or download newer virus definitions and scan again.
   - Quarantine If Unrepairable: Attempts a repair of an infected file automatically. If the repair is not successful, the virus-infected file is isolated in the Quarantine.
4. Click OK to save your settings and close the Options dialog box.

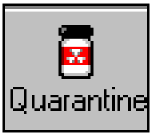
Quarantine infected or suspicious files

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

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

- You selected Quarantine after receiving a Norton AntiVirus alert.
- You open the Quarantine and click Add Item to manually select a file and add it to the Quarantine.

- Norton AntiVirus is configured to quarantine infected items rather than repair them or to quarantine them if they cannot be repaired.



To re-scan a file isolated in the Quarantine:

1 Start Norton AntiVirus.

2 Click the Quarantine button in the Norton AntiVirus main window.

3 Click LiveUpdate in the Quarantine window.

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

4 Select the file in the Quarantine and click Repair Item.

The file is scanned again with the new definitions.

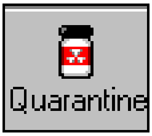
Submit a potentially infected file to SARC for analysis

WHY? Sometimes Norton AntiVirus detects an unknown virus that can't be eliminated. Or, you have a file you think is infected that is not being detected. The Symantec AntiVirus Research Center (SARC) will analyze your file to make sure it is not infected. If a new virus is discovered in your submission, SARC will create and send you special updated virus definitions to detect and eliminate the new virus.

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

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

You must have an Internet connection to submit a sample and an email address to receive a reply.



To submit a file to SARC:

1 Start Norton AntiVirus.

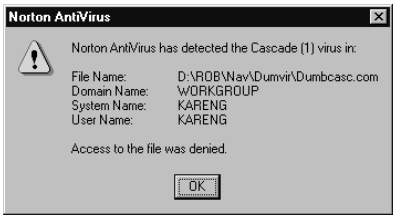
2 Click the Quarantine button in the Norton AntiVirus main window.

3 Select a file in the list of Quarantined items and click Submit Item.

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

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

What to do if a virus is found



Norton AntiVirus

Norton AntiVirus has detected the Cascade (1) virus in:

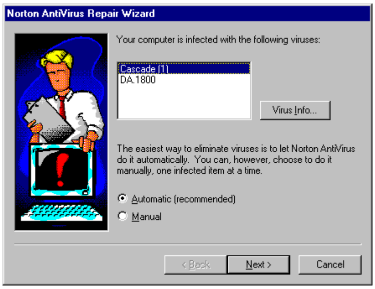
File Name:	D:\ROB\Nav\Dumvir\Dumbcasc.com
Domain Name:	WORKGROUP
System Name:	KARENG
User Name:	KARENG

Access to the file was denied.

If you see a virus alert

1. As part of Auto-Protect operation, Norton AntiVirus is preset to Deny Access to an infected file during regular computer operation. This means that you can't run an infected program or open an infected document.
2. Start Norton AntiVirus and scan your disk to eliminate the virus. See "Scan for viruses" on page 17.

You can also configure Auto-Protect to either Repair or Delete an infected file automatically. See "Change how Auto-Protect works" on page 20.



Norton AntiVirus Repair Wizard

Your computer is infected with the following viruses:

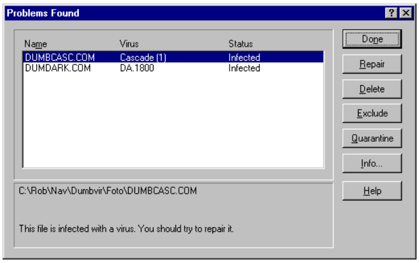
Cascade (1)
DA.1800

The easiest way to eliminate viruses is to let Norton AntiVirus do it automatically. You can, however, choose to do it manually, one infected item at a time.

● Automatic (recommended)
○ Manual

If you see the Repair Wizard

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



Problems Found

Name	Virus	Status
DUMBCASC.COM	Cascade (1)	Infected
DUMDARK.COM	DA.1800	Infected

C:\Rob\Nav\Dumbvir\Foto\DUMBCASC.COM

This file is infected with a virus. You should try to repair it.

If you see the Problems Found dialog

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

See "Quick guide to alert actions" on page 24 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.

Actions	When and why you use them
Repair	For a virus found, Repair is always the best choice. Repair eliminates the virus and repairs the infected item automatically.
Delete	Deletes (erases) the infected file—both the infected file and the virus are gone forever. Replace a deleted file with a backup copy. Reinstall a deleted program from the original program disks. If the virus is detected again, your backup copy or original program disks are infected.
Stop	Stops a scan from continuing.
Continue	Ignores the virus detected and continues the scan.
Exclude	Ignores the virus detected and excludes the file from checks for known viruses during future scans. Choose Exclude only if you do not want the file checked again.
Quarantine	Isolates the virus-infected file, but does not remove the virus. Choose Quarantine if you suspect the infection is caused by an unknown virus and you want to submit the virus to the Symantec AntiVirus Research Center for analysis.

What to do if NortonAntiVirus can’t repair

WHY? One of the most common reasons Norton AntiVirus can’t repair a file is that you don’t have the most up-to-date virus protection files.

Do one of the following:

- Update your virus protection and scan again. See page 28 for details.
- Read the information on your screen carefully to identify the type of item that can’t be repaired, then match it to one of the types below:
  - Infected files are those with filenames that include .COM or .EXE. Document files such as .DOC, .DOT, and .XLS can also be infected.
  - Compressed files may contain many files. You can often tell a compressed file by its name. Many compressed files end in .ZIP.
  - Hard disk master boot record, boot record, or system files are replaced using your Windows NT system disks.

Infected files

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

If Norton AntiVirus can’t repair a file:

Do one of the following:

- Choose Quarantine.

  After the file is quarantined, you can update you virus definitions and scan again or submit the file to SARC for analysis. For more information, see “Quarantine infected or suspicious files” on page 21 and “Submit a potentially infected file to SARC for analysis” on page 22.

- Choose Delete.

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

Compressed files

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

To uncompress and repair:

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

Hard disk master boot record or boot record

If Norton AntiVirus could not successfully repair the master boot record or a boot record on your hard disk, restart your computer from the Windows NT Emergency Repair Disk that you created when you installed Windows to attempt a repair. If this fails, you will have to reinstall Windows NT.

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.

Keeping virus protection current

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

How to update virus protection

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

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

Updating virus protection with LiveUpdate

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

To update virus protection:

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

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

4. Click Next to start the automatic update.

Using LiveUpdate Email

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

To receive LiveUpdate Email:

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

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

To start a LiveUpdate session from the LiveUpdate Email:

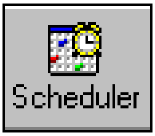
- When you receive a LiveUpdate Email, launch or run the email attachment called LIVEUPDT.NLU from your mail program.

  You must launch or run the attachment. Simply reading or viewing it will not work.

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

Scheduling automatic LiveUpdates

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



To schedule automatic LiveUpdates:

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click Scheduler.
3. Click Add.
4. Select Scheduled LiveUpdate for the Type Of Event.

5. Select Monthly for the Frequency.
6. Click OK to close the dialog box, then click OK again to confirm.
7. Click the Exit button in the upper-right corner of the Norton Scheduler dialog box.

   Your computer must be on when the LiveUpdate is due to take place.

Updating virus protection without LiveUpdate

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

To install the latest virus definitions:

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

   The Intelligent Updater program searches your computer for Norton AntiVirus, then installs the new virus definitions files in the proper folder automatically.
4. Restart your computer.
5. Scan your disk to make sure newly discovered viruses are detected.

Troubleshooting

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

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

The virus may be in a program file with an unusual extension that Norton AntiVirus isn't set to look for. Do this:

1 Start Norton AntiVirus.

2 Click the Options button in the Norton AntiVirus main window.

3 Click the Scanner tab.

4 Select the All Files option in the What To Scan group.

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

6 Scan all disks that you use and repair all infected files.

The source of the infection may be a floppy disk. Scan all the floppy disks you use for viruses.

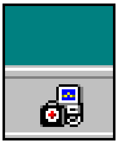
Norton AntiVirus can't repair my infected files.

The main reason that Norton AntiVirus may not be able to repair your infected files is you don't have the latest virus definitions files installed on your computer. You should update these files regularly to protect your computer from the latest viruses. To update virus definitions, see page 28.

A program does not work properly after repair.

Although Norton AntiVirus removes the virus, the file may be damaged beyond repair. Delete the program and replace it with a backup copy or reinstall it from the original program disks. If the virus is detected again, the backup copy or original program disks are probably infected.

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



If the Norton AntiVirus Auto-Protect icon does not appear in the lower-right corner of the taskbar on your Windows desktop, Auto-Protect is not loaded. The likely reason this is happening is Norton AntiVirus is not configured to start Auto-Protect automatically. Do this:

1. Start Norton AntiVirus.
2. Click the Options button in the Norton AntiVirus main window.
3. Click the Auto-Protect tab.
4. Check the Load Auto-Protect At Startup check box.
5. Click OK to save your settings and close the Options dialog box.

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

Do one of the following:

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

Command-line switches

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

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

```
NAVWNT [pathname] [options]
```

`pathname`	Any drive, folder, file, or combination of these is scanned. To scan multiple items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files; for example, NAVWNT A: C:\MYDIR\*.EXE
`/A`	All drives, except drives A: and B:, are scanned. Network drives are scanned if the Allow Network Scanning option is selected in the Scanner Advanced Settings dialog box.
`/L`	All local drives, except drives A: and B:, are scanned.
`/S[+|-]`	Enables (+) or disables (-) scanning of subfolders for any folders specified in the pathname. S+ is the default.
`/B[+|-]`	Enables (+) or disables (-) scanning of boot records; for example, NAVWNT A: /B+ or NAVWNT A: /B- (default is the Scanner options setting).
`/BOOT`	Only the boot records of the specified drives are scanned.
`/NORESULTS`	No scan results are reported on screen.

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

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

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

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

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

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

  ```
  NAVWNT "C:\Program Files"
  ```

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

  ```
  NAVWNT C: D:\NEWFILES
  ```

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

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

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

  ```
  NAVWNT C: A: /BOOT
  ```

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

  ```
  at 17:30 /interactive /every:M,T,W,Th,F
  "C:\Program Files\NAVNT\NAVWNT" /L /NORESULTS
  ```

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

Potential Virus Submission Procedure

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

Symantec AntiVirus Research Center
2500 Broadway, Suite 200
Santa Monica, CA 90404

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

Please provide the following information:

Operating System:

□ DOS (version _______)   □ Windows 95/98   □ Windows NT   □ Windows 3.x

Have you loaded the most recent virus definitions?

□ Yes (date of VIRSCAN.INF file ____________)   □ No (date of VIRSCAN.INF file ____________)

Has any other scanner identified a virus?

□ Yes (name and version of scanner ________________________ virus reported_______________)   □ No

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

____

____

____

____

____

____

____

Your Name____

Company Name ____

Street Address ____

City ____________________________________ State _______ Zip/Postal Code ________________

Country__________________________ Daytime Phone ______________________________

Fax ________________________ Email Address ____________________________________

SYMANTEC.™

Creating a Virus Sample Floppy Disk

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

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

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

To create a virus sample floppy disk:

1 Start the potentially infected system from its own hard drive.

Windows 95/98: Press function key F8 before Windows starts and choose “Safe mode command prompt only” from the on-screen menu.

2 Format a floppy disk with the potentially infected operating system.

From the DOS prompt, type `FORMAT A: /S` and press Enter.

3 Do one of the following:

- Windows 3.1/DOS: Copy MODE.COM, MEM.EXE, KEYB.COM, and XCOPY.EXE from your C:\DOS folder to the floppy disk.
- Windows 95/98: Copy MODE.COM, MEM.EXE, KEYB.COM, and XCOPY.EXE from your C:\WINDOWS\COMMAND folder to the floppy disk.
- Windows NT: Copy COMMAND.COM, CMD.EXE, MODE.COM, MEM.EXE, and MORE.EXE from \Winnt\system32 to the floppy disk.

4 Type `A:` and press Enter to change to the A: drive.

5 Type `PATH;` and press Enter (don’t forget the semicolon) to remove the path from the environment temporarily.

6 Run the programs (ignore any screen messages). The engineers will be able to determine if they become infected. For example,

- Type `A:MODE` and press Enter.
- Type `A:MEM` and press Enter.
- Type `A:XCOPY` and press Enter.

7 Program viruses: Copy any files that you suspect are infected to the floppy disk in the A: drive.

Word macro viruses: Copy any documents that you suspect are infected, along with NORMAL.DOT from the TEMPLATE directory, to the floppy disk in the A: drive.

Excel macro viruses: Copy any worksheets that you suspect are infected, along with any files in the XLSTART directory, to the floppy disk in the A: drive..

8 Label the floppy disk with your name, address, telephone number, and the date of its creation. Write “Potential Virus” on the disk label.

9 Complete and send the form on the previous page with the floppy disk to Symantec.

INDEX