Norton Internet Security™
User's Guide

Norton

2002

Internet Security™

Norton Internet Security™ 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.

Documentation version 4.0

PN: 07-30-00467

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 changes without prior notice.

Standard Template Library

This product utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators.

Trademarks

Symantec, the Symantec logo, Norton, Norton Internet Security, Norton Personal Firewall, 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. 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 or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. License.

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. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.

B. 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;

C. 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; and

D. 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 license.

You may not:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. 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;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

F. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. 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 (60) day period following the delivery to you of the Software.

4. 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 OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

5. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR

INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS 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.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

6. U.S. Government Restricted Rights:

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

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 175 W. Broadway, Eugene, OR 97401, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

This product utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright © 1994. Hewlett-Packard Company.

How to minimize Internet risks

Install Norton Internet Security

For more information, see “Installing Norton Internet Security” on page 19.

Run LiveUpdate weekly to keep protection current

For more information, see “Getting started with Norton Internet Security” on page 35.

Set up access restrictions for children and teens

For more information, see “Controlling access to Web content” on page 53.

Identify private information to safeguard

For more information, see “Protecting confidential information” on page 71.

Respond appropriately to Norton Internet Security alerts

For more information, see “Responding to Norton Internet Security alerts” on page 81.

Customize firewall protection

For more information, see “Customizing firewall protection” on page 93.

Keep Norton Internet Security protection enabled

For more information, see “Customizing firewall protection” on page 93.

Keep Norton AntiVirus protection enabled

For more information, see Norton AntiVirus Help.

CONTENTS

How to minimize Internet risks

Chapter 1 Introducing Norton Internet Security

Chapter 2 Installing Norton Internet Security

Chapter 3 Getting started with Norton Internet Security

Chapter 4 Controlling access to Web content

Chapter 5 Protecting confidential information

Chapter 6 Blocking Internet advertisements

Chapter 7 Responding to Norton Internet Security alerts

Chapter 8 Customizing firewall protection

Chapter 9 Handling virus emergencies

Chapter 10 Monitoring Norton Internet Security events

Chapter 11 Configuring Norton Internet Security for common situations

Chapter 12 Troubleshooting

Appendix A About the Internet

Appendix B Understanding Internet risks

Service and support solutions

CD Replacement Form

Index

CHAPTER 1

Introducing Norton Internet Security

Millions of computers connect to the Internet, and the number increases daily. When you are connected to the Internet, you can connect with millions of other computers and those computers can connect with your computer. Unprotected connections to the Internet leave your computer vulnerable to hacker attacks, viruses, Trojan horses, and other Internet threats.

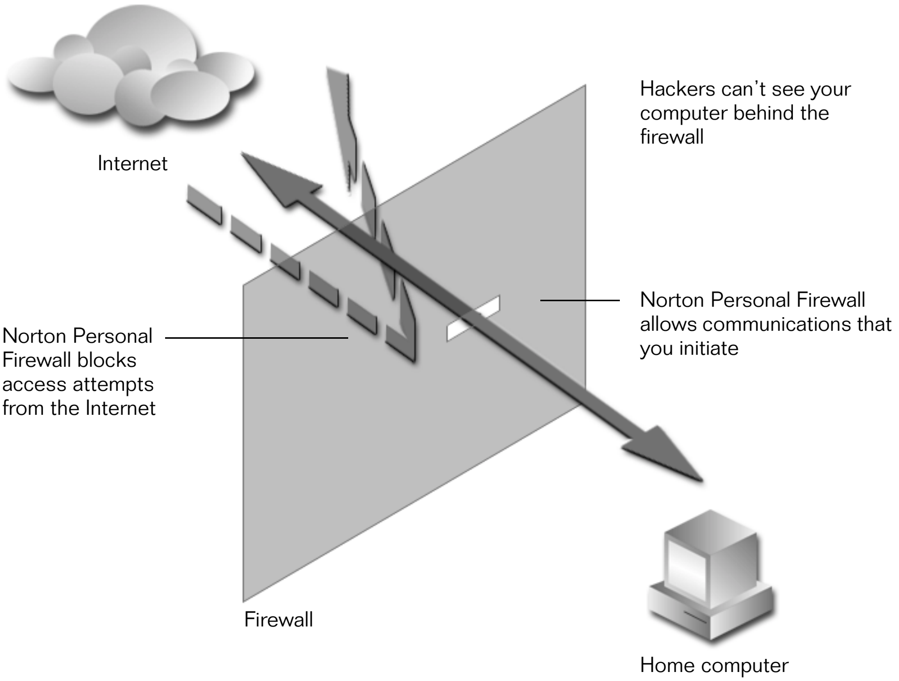
Norton Internet Security includes several components that work together to protect you from Internet threats and enhance your Internet experience in the following ways:

- Prevents unauthorized access to your computer when you are on the Internet
- Protects your personal information
- Blocks Internet advertisements to speed your Internet browsing
- Protects your family from inappropriate content
- Provides comprehensive virus protection, detection, and elimination

Preventing unauthorized access

Norton Internet Security includes Norton Personal Firewall, which provides a barrier between your computer and the Internet. A *firewall* prevents unauthorized access to or from a computer or network. Firewalls prevent unauthorized Internet users from accessing private computers and networks connected to the Internet.

Norton Personal Firewall uses rules to determine whether to permit or block connections. You can change these rules, permitting or blocking applications from having Internet access.


Internet
Hackers can't see your computer behind the firewall
Norton Personal Firewall allows communications that you initiate
Norton Personal Firewall blocks access attempts from the Internet
Firewall
Home computer

Norton Personal Firewall can automatically determine the best way to protect many applications. When an application that Norton Personal Firewall does not recognize attempts to communicate over the Internet, Norton Personal Firewall alerts you, and helps you determine if Internet access is appropriate for that application.

ActiveX controls and *Java applets* are applications that run in your browser. While most of these applications are useful, some are harmful. Norton Personal Firewall can be configured to prevent ActiveX controls and Java applets from running without your knowledge, and lets you specify sites on which these applications can run.

Protecting personal information

You may not want confidential information, such as credit card numbers or your home phone number, to be sent unencrypted over the Internet. Privacy Control prevents confidential information from being sent over nonsecure connections to Web sites or through instant messenger programs.

Cookies are small files stored on your computer that Web sites use to track your Web usage. Norton Internet Security can block cookies and other information that your browser normally reports to Web sites, such as the address of the previous Web site that you visited and the type of Web browser you are using.

You may want to prevent some users in your household from ever sending confidential information over the Internet. Norton Internet Security can block users from accessing secure sites on which they may be asked for personal information.

Controlling access to Web content

With Parental Control, parents can control which Web sites their children visit. Parents can also control which types of applications their children use to access the Internet, effectively blocking Internet access to chat software or other applications.

Because members of your family may have different Internet use requirements, you can create as many user accounts as you need. Each account can have a unique level of protection. Parental Control helps you set up accounts with controls appropriate for children, teenagers, and adults.

Blocking Internet advertisements

Norton Internet Security can block banner ads, pop-up windows, and other clutter on Web pages, making Web browsing faster and more enjoyable.

Comprehensive virus protection

Norton Internet Security includes Norton AntiVirus, which is an important component of your Internet protection. It automatically protects against viruses, Trojan horses, and malicious ActiveX controls and Java applets.

Online assistance

Norton Internet Security provides extensive online assistance.

- The Security Assistant is a wizard that introduces you to Norton Internet Security and helps you select the correct settings to maximize your protection. After you install Norton Internet Security and restart your computer, the Security Assistant appears. The Security Assistant is always available to provide information about how Norton Internet Security works, or to change any of the settings you selected.
- Online Help is a comprehensive reference to Norton Internet Security. It includes a table of contents, a comprehensive index, and full-text search capabilities, making it easy to find the information you need.
- In most windows and dialog boxes, Tell Me More or Help is available to provide specific information about where you are in Norton Internet Security.
- What's This? Help provides a quick definition of an individual component of a window or dialog box.

Tips for safe computing

Norton Internet Security provides many of the tools you need to minimize Internet risks. Other things you can do to ensure safe Internet use include:

- Keep your browser up-to-date. Software publishers release new versions to fix vulnerabilities that have been found in their browsers.
- Use passwords intelligently. For important information, use complex passwords that include capital and lowercase letters, numbers, and symbols. Don't use the same password in multiple places.
- Don't run software if you don't trust the publisher and the source from which you received the software.
- Don't open email attachments unless you are expecting the attachment and you trust the sender.

- Be sensible about providing personal information where it isn't warranted. Many sites ask for more information than they need.
- Review the privacy policies of the sites to which you are considering sending information.

For more information, see “Understanding Internet risks” on page 151.

CHAPTER 2

Installing Norton Internet Security

Before installing Norton Internet Security, take a moment to review the system requirements listed in this chapter. Windows 98 and Windows Me users should have some blank 1.44-MB disks available to make Rescue Disks.

System requirements

To use Norton Internet Security, your computer must have one of the following Windows operating systems:

- Windows 98, 98SE
- Windows Me
- Windows NT v4.0 Workstation operating system with Service Pack 6a or higher
- Windows 2000 Professional Workstation
- Windows XP Professional or Windows XP Home Edition

Your computer must also meet the following minimum requirements.

Windows 98/Me

- Intel Pentium processor at 150 MHz
- 32 MB of RAM
- 60 MB of available hard disk space without Parental Control installed; 90 MB with Parental Control
- Internet Explorer 4.01 Service Pack 1 or higher
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

Windows NT 4.0 Workstation

- Service Pack 6a or higher
- Intel Pentium processor at 150 MHz
- 64 MB of RAM
- 60 MB of available hard disk space without Parental Control installed; 90 MB with Parental Control
- Internet Explorer 4.01 Service Pack 1 or higher
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

Windows 2000 Professional Workstation

- Intel Pentium processor at 150 MHz
- 64 MB of RAM
- 60 MB of available hard disk space without Parental Control installed; 90 MB with Parental Control
- Internet Explorer 4.01 Service Pack 1 or higher
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

Windows XP Home Edition/Professional

- Intel Pentium processor at 300 MHz or higher
- 128 MB of RAM
- 60 MB of available hard disk space without Parental Control installed; 90 MB with Parental Control
- Internet Explorer 4.01 Service Pack 1 or higher
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

Before installation

If you are using Windows XP, disable the XP firewall.

Before you install Norton Internet Security, prepare your computer and, if you have a computer that cannot start from a CD, create Emergency Disks.

Preparing your computer

If you have previous versions of Norton Internet Security or any anti-virus programs on your computer, you must uninstall them before installing Norton Internet Security. For more information, see “If you need to uninstall Norton Internet Security” on page 32.

To uninstall other anti-virus programs, see the user documentation that came with the program.

You must also quit all other Windows programs before installing Norton Internet Security.

Creating Emergency Disks

Emergency Disks are used to start your computer and scan for viruses in case of a problem. If your computer can start from a CD, you can use the Norton Internet Security CD in place of Emergency Disks and do not need to create them. For more information, see "Using Emergency Disks in virus emergencies" on page 115.

Use the Norton Internet Security CD to create Emergency Disks. You will need three formatted 1.44-MB disks.

Note: If you cannot start your computer, you can use these instructions to create Emergency Disks on another computer.

To create Emergency Disks

1. Insert the Norton Internet Security CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Open the Support folder.
4. Open the Edisk folder.
5. Double-click **Ned.exe**.
6. In the welcome window, click **OK**.
7. Label the first disk as instructed, insert it into drive A and click **Yes**.
8. Repeat step 7 for the second and third disks.
9. Click **OK** when the procedure is complete.
10. Remove the third disk from drive A and store the Emergency Disk set in a safe place.

Installation

Install Norton Internet Security from the Norton Internet Security CD.

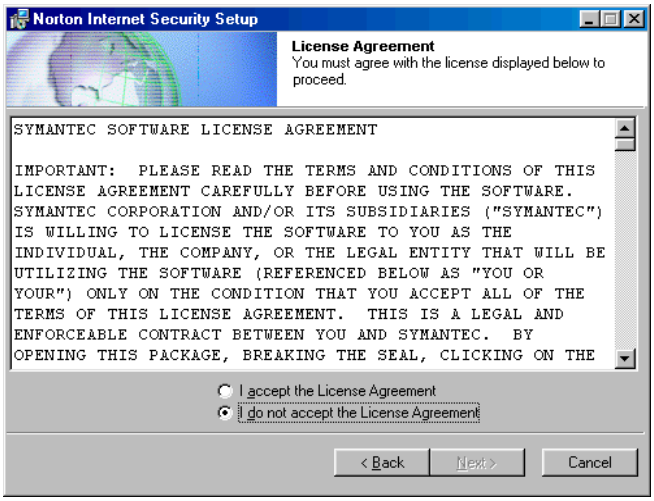
To install Norton Internet Security

1 Insert the Norton Internet Security CD into the CD-ROM drive.

2 In the Norton Internet Security CD window, click **Install Norton Internet Security**.

If your computer is not set to automatically open a CD, you will have to open it yourself. For more information, see "If the opening screen does not appear" on page 27.

3 The first installation window reminds you to close all other Windows programs. Click **Next**.



Norton Internet Security Setup

License Agreement

You must agree with the license displayed below to proceed.

```
SYMANTEC SOFTWARE LICENSE AGREEMENT

IMPORTANT:  PLEASE READ THE TERMS AND CONDITIONS OF THIS
LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC")
IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE
INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE
UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR
YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE
TERMS OF THIS LICENSE AGREEMENT.  THIS IS A LEGAL AND
ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC.  BY
OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE
```

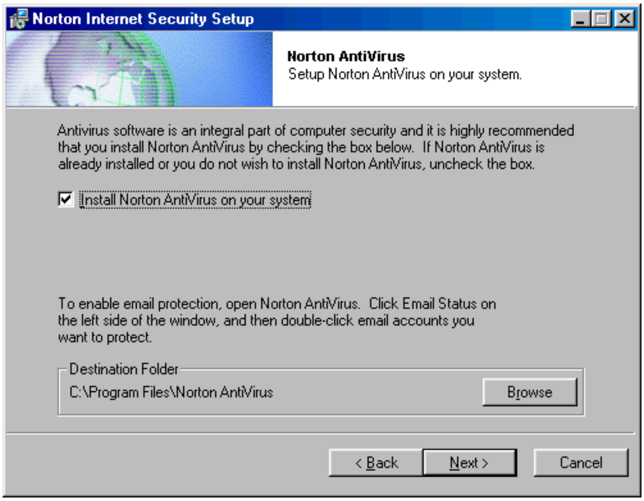
○ I accept the License Agreement

● I do not accept the License Agreement

4 In the License Agreement window, click **I accept the License Agreement**.

If you decline, you cannot continue with the installation.

5 Click **Next**.



Norton AntiVirus
Setup Norton AntiVirus on your system.

Antivirus software is an integral part of computer security and it is highly recommended that you install Norton AntiVirus by checking the box below. If Norton AntiVirus is already installed or you do not wish to install Norton AntiVirus, uncheck the box.

☑ Install Norton AntiVirus on your system

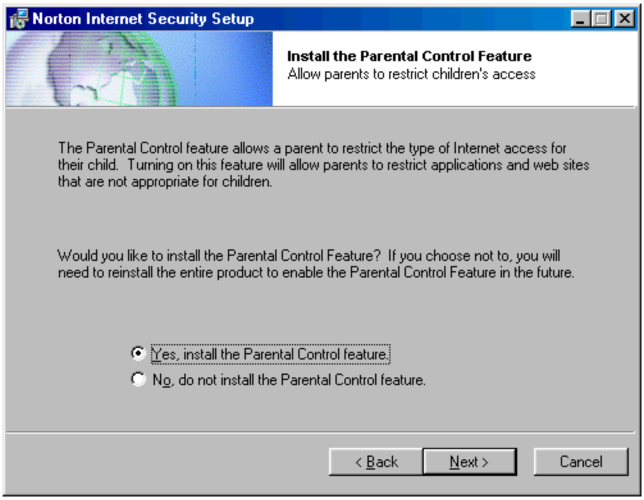
To enable email protection, open Norton AntiVirus. Click Email Status on the left side of the window, and then double-click email accounts you want to protect.

Destination Folder: C:\Program Files\Norton AntiVirus

6 Norton AntiVirus is included as part of Norton Internet Security. To install it, check **Install Norton AntiVirus on your system** and click **Browse** to specify the location to which you want it installed.

If a later version of Norton AntiVirus is already on your computer, you will not see this window.

7 Click **Next**.



Install the Parental Control Feature
Allow parents to restrict children's access

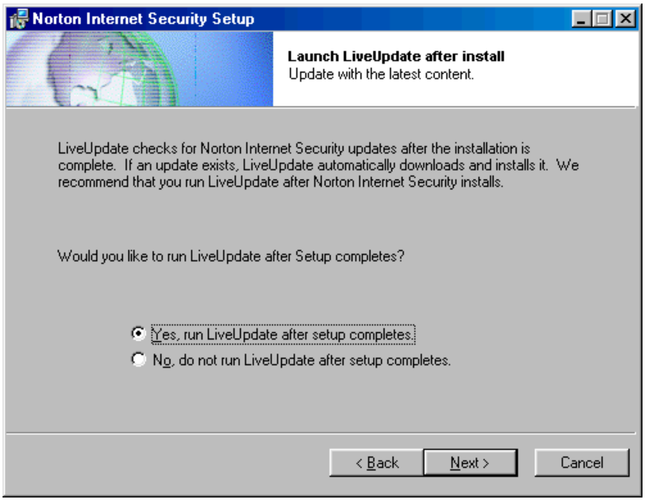
The Parental Control feature allows a parent to restrict the type of Internet access for their child. Turning on this feature will allow parents to restrict applications and web sites that are not appropriate for children.

Would you like to install the Parental Control Feature? If you choose not to, you will need to reinstall the entire product to enable the Parental Control Feature in the future.

● Yes, install the Parental Control feature.
○ No, do not install the Parental Control feature.

8 The Parental Control feature lets you restrict Internet access for any children using your computer. Select whether or not you want to install the Parental Control feature.

9 Click **Next**.



Launch LiveUpdate after install
Update with the latest content.

LiveUpdate checks for Norton Internet Security updates after the installation is complete. If an update exists, LiveUpdate automatically downloads and installs it. We recommend that you run LiveUpdate after Norton Internet Security installs.

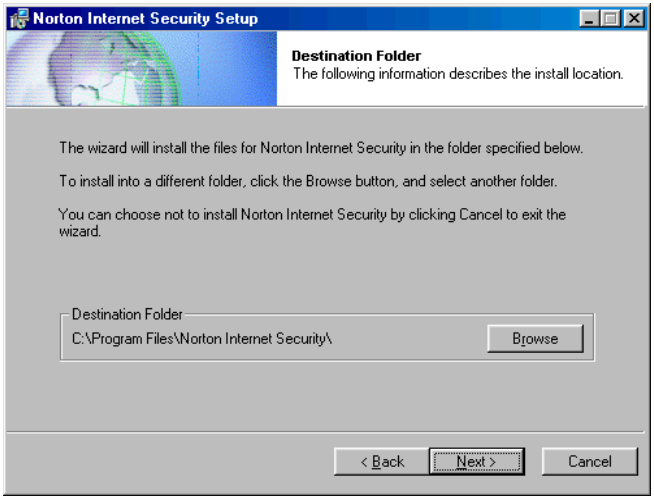
Would you like to run LiveUpdate after Setup completes?

● Yes, run LiveUpdate after setup completes.

○ No, do not run LiveUpdate after setup completes.

10 LiveUpdate keeps your copy of Norton Internet Security up to date with the latest program and protection updates. Select whether or not you want to run LiveUpdate after installation is done.

11 Click **Next**.



Destination Folder
The following information describes the install location.

The wizard will install the files for Norton Internet Security in the folder specified below.

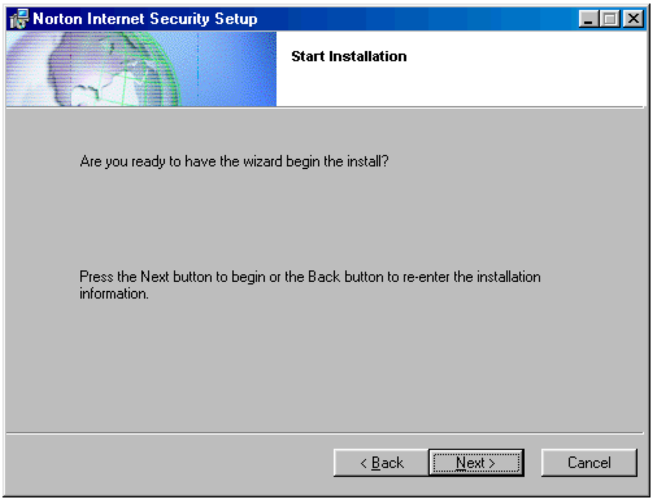
To install into a different folder, click the Browse button, and select another folder.

You can choose not to install Norton Internet Security by clicking Cancel to exit the wizard.

Destination Folder
C:\Program Files\Norton Internet Security\

12 Click **Browse** to select a folder into which you want Norton Internet Security installed, if other than the default location.

13 Click **Next**.



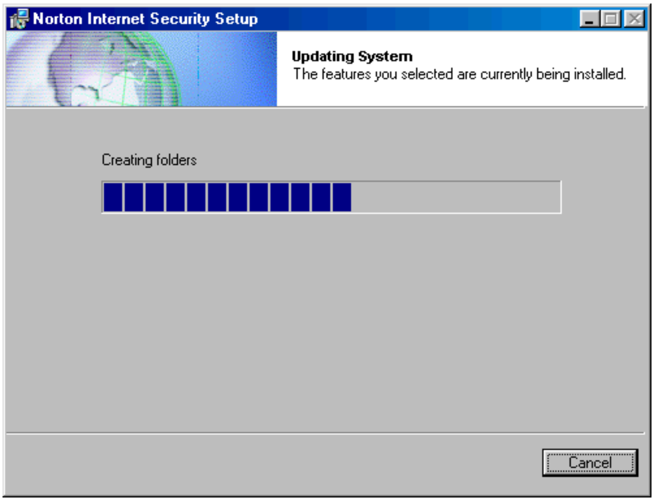
Norton Internet Security Setup

Start Installation

Are you ready to have the wizard begin the install?

Press the Next button to begin or the Back button to re-enter the installation information.

14 Click **Next** to begin installing Norton Internet Security.



Norton Internet Security Setup

Updating System

The features you selected are currently being installed.

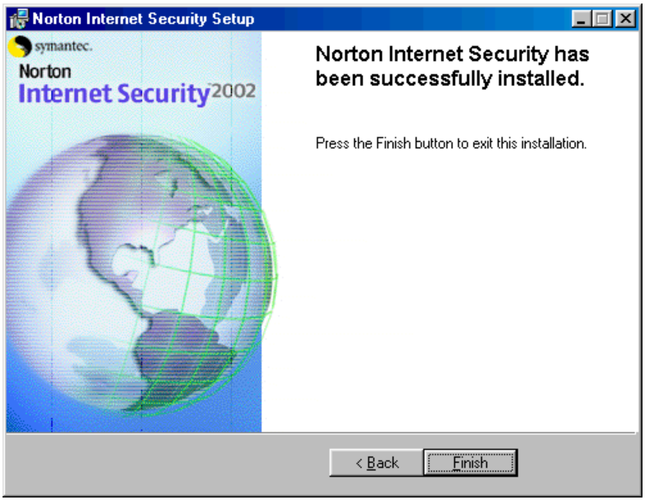
Creating folders

After Norton Internet Security is installed, the Registration Wizard appears with which you can register your software. For more information, see "Registering your software" on page 28.

If you chose to run LiveUpdate after installation, it runs after registration.

15 When LiveUpdate is done, click **Finish**.

16 Scroll through the Readme text, then click **Next**.



Norton Internet Security has been successfully installed.

Press the Finish button to exit this installation.

17 Click **Finish** to exit the installation.

If the opening screen does not appear

Sometimes, a computer's CD-ROM drive does not automatically start a CD.

To start the installation from the Norton Internet Security CD

1 On your desktop, double-click **My Computer**.

2 In the My Computer dialog box, double-click the icon for your CD-ROM drive.

3 From the list of files, double-click **CDSTART.EXE**.

Registering your software

Use the Registration Wizard to register your software online. If you skip online registration, you can register your software later using the Product Registration option on the Help menu.

To register your software

1. In the first Registration window, select the country from which you are registering and the country in which you live (if different), then click **Next**.
2. If you would like information from Symantec about Norton Internet Security, select the method by which you want to receive that information, then click **Next**.
3. Type your name and whether you want Norton Internet Security registered to you or your company, then click **Next**.
4. Type your address, then click **Next**.
5. Do one of the following:
   - Answer the survey questions to help Symantec improve its products and services, then click **Next**.
   - Skip the survey by clicking **Next**.
6. Select whether you want to register Norton Internet Security through the Internet or by mail.
   - If you want to register by mail, your computer must be connected to a printer that the Registration Wizard can use to print the registration form.
   - If you want to register using the Internet, you must be connected to the Internet.
7. Click **Next**.

   If you submitted your registration through the Internet, the Registration Wizard displays the serial number for your product.
8. Write down the serial number or click **Print** to get a copy of your registration information for future reference.
9. Click **Next**.
10. Select whether you want to use your existing profile the next time you register a Symantec product, or type the information as part of registration.
11. Click **Finish**.

After installation

If your computer needs to be restarted after Norton Internet Security is installed, a prompt appears giving you the option to do so immediately. After restart or, if your computer does not need to be restarted, after installation is complete, the Information Wizard appears. After you complete the Information Wizard, the Security Assistant appears to walk you through the configuration of Norton Internet Security.

Note: If you bought your computer with Norton Internet Security already installed, the Information Wizard appears the first time you start the product. You must accept the license agreement that appears in the Information Wizard for Norton Internet Security to be activated.

Restarting your computer

After installation, you may receive a prompt telling you that your computer needs to be restarted for the updates to take effect.

To restart your computer

- In the Installer Information dialog box, click **Yes**.

  If you click No, configuration of Norton Internet Security is not complete until you restart your computer.

Using the Information Wizard

The Information Wizard gives you information about the Symantec subscription service.

To use the Information Wizard

1 On the Welcome screen, click **Next**.

If you purchased your computer with Norton Internet Security already installed, you must accept the license agreement in order to use Norton Internet Security. You can then register your software.

2 Click **I accept the license agreement**, then click **Next**.

The Registration Wizard appears, with which you can register online. For more information, see “Registering your software” on page 28.

When you have completed registration, information about your subscription appears.

3 Review the subscription service information, then click **Next**.

If you purchased your computer with Norton Internet Security already installed, you have the option to disable Parental Control. For more information, see “Controlling access to Web content” on page 53.

4 Select whether or not you want to disable Parental Control, then click **Next**.

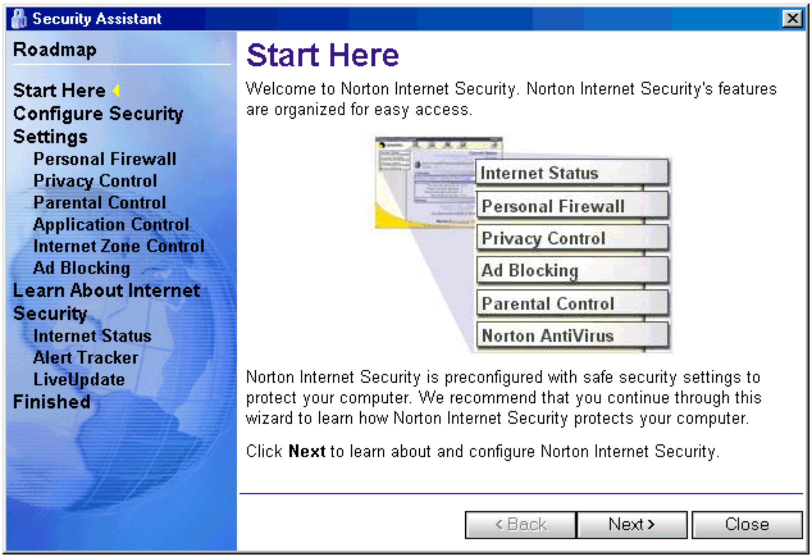
If you purchased your computer with Norton Internet Security already installed, the Readme file appears.

5 Scroll through the Readme, then click **Next**.

6 On the final Information Wizard screen, click **Finish**.

Using the Security Assistant

The Security Assistant begins automatically after you have completed the Information Wizard. You can use it to review and, if desired, change how Norton Internet Security has been configured for your computer.



Start Here

Welcome to Norton Internet Security. Norton Internet Security's features are organized for easy access.

Norton Internet Security is preconfigured with safe security settings to protect your computer. We recommend that you continue through this wizard to learn how Norton Internet Security protects your computer.

Click **Next** to learn about and configure Norton Internet Security.

Note: It is recommended that you use the default settings for Norton Internet Security. If you discover that changes need to be made after you have worked with Norton Internet Security for a while, you can use the Security Assistant to make those changes. For more information, see “Using the Security Assistant” on page 44.

To use the Security Assistant

- At the bottom of each pane, click **Next** to progress through the Security Assistant and review all settings.
- In the Roadmap on the left side of the Security Assistant window, click the name of a feature to review the settings for that feature.
- Click **Close** to close the Security Assistant.

If you have Norton SystemWorks installed

If you have Norton SystemWorks installed on your computer when you install Norton Internet Security, after you step through the Information Wizard you are asked if you want to integrate Norton Internet Security with Norton SystemWorks. If you click Yes, three things happen:

- A Norton Internet Security tab appears in the Norton SystemWorks main window. All Norton Internet Security features appear when you click the tab.
- Norton Internet Security appears as a tool in the Norton Tray Manager.
- If you attempt to open Norton Internet Security, Norton SystemWorks opens instead.

If you need to uninstall Norton Internet Security

If you need to remove Norton Internet Security from your computer, use the Uninstall Norton Internet Security option on the Windows Start menu. You can uninstall only the Norton AntiVirus component of Norton Internet Security if you want.

Note: During uninstall, Windows may indicate that it is installing software. This is a general Microsoft installer message and can be disregarded.

To uninstall Norton Internet Security

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Uninstall Norton Internet Security**.
   - On the Windows XP taskbar, click **Start** > **More Programs** > **Norton Internet Security** > **Uninstall Norton Internet Security**.
2. Do one of the following:
   - Click **Remove NAV** to uninstall the Norton AntiVirus component of Norton Internet Security.
   - Click **Remove All** to uninstall the entire product.
3. Click **Next**.

4 If you have files in Quarantine, you are asked if you want to delete them. Select one of the following:
   - Yes: Deletes the quarantined files from your computer.
   - No: Leaves the quarantined files on your computer, but makes them inaccessible. To repair or submit the files to Symantec for analysis, reinstall Norton Internet Security.

5 In the Installer Information dialog box, click **Yes** to restart your computer.

If you have no other Symantec products on your computer, you should also uninstall LiveReg and LiveUpdate.

To uninstall LiveReg and LiveUpdate

1 Do one of the following:
   - On the Windows taskbar, click **Start > Settings > Control Panel**.
   - On the Windows XP taskbar, click **Start > Control Panel**.

2 In the Control Panel, double-click **Add/Remove Programs**.

3 In the list of currently installed programs, click **LiveReg**.

4 Do one of the following:
   - In Windows 2000 or Windows Me, click **Change/Remove**.
   - In Windows 98 or Windows NT, click **Add/Remove**.
   - In Windows XP, click **Remove**.

5 Click **Yes** to confirm that you want to uninstall the product.

Repeat steps 1 through 5, selecting LiveUpdate in step 3, to uninstall LiveUpdate.

CHAPTER 3

Getting started with Norton Internet Security

Norton Internet Security starts automatically when you restart your computer. You do not have to open the program to be protected.

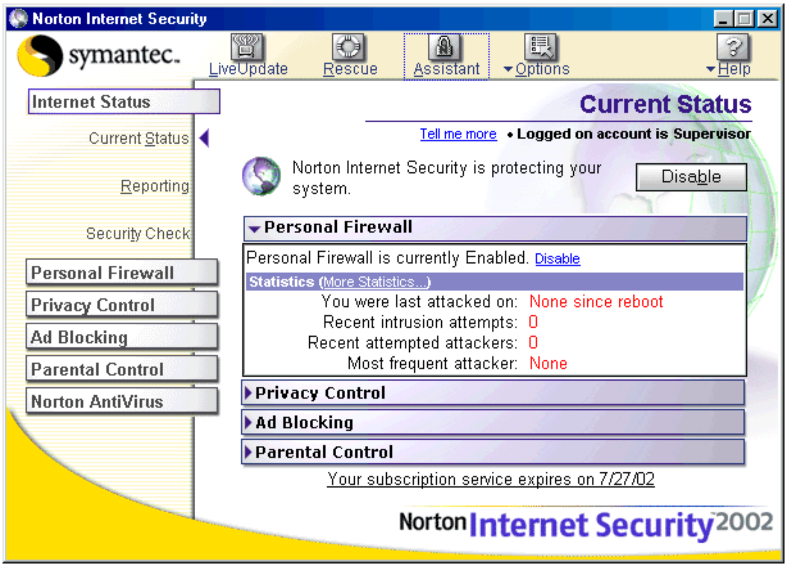
Starting Norton Internet Security

Start Norton Internet Security if you want to change protection settings or monitor the activities of the program.

To start Norton Internet Security

- Do one of the following:
  - In the notification area of the Windows taskbar, double-click **Norton Internet Security**.
  - On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Norton Internet Security**.
  - On the Windows XP taskbar, click **Start > More Programs > Norton Internet Security > Norton Internet Security**.
  - On the Windows desktop, double-click **Norton Internet Security**.

The Norton Internet Security main window appears.



• Logged on account is Supervisor

Norton Internet Security is protecting your system.

Personal Firewall is currently Enabled.

You were last attacked on: None since reboot
Recent intrusion attempts: 0
Recent attempted attackers: 0
Most frequent attacker: None

Your subscription service expires on 7/27/02

Temporarily disabling Norton Internet Security

There may be times when you want to temporarily suspend a protection feature or the entire product. For example, you might want to see if Norton Internet Security is preventing a Web page from appearing correctly. Norton Internet Security lets you turn features off without adjusting the settings.

To temporarily disable Norton Internet Security

1 On the left side of the Norton Internet Security window, click **Internet Status > Current Status**.

Make sure you are logged on to Norton Internet Security using an account with Adult or Supervisor rights. Restricted accounts cannot disable any portion of Norton Internet Security. For more information, see “Logging on and logging off” on page 68.

2 In the Current Status window, click **Disable**.

You can also disable Norton Internet Security by right-clicking the Norton Internet Security icon in the notification area of the Windows taskbar and clicking Disable.

Norton Internet Security is enabled when you click Enable or the next time you start your computer.

Disabling a protection feature

You can disable a protection feature. For example, you might want to see if the Personal Firewall is preventing an application from operating correctly.

To disable a protection feature

1 On the left side of the Norton Internet Security window, click **Internet Status** > **Current Status**.

  Make sure you are logged on to Norton Internet Security using an account with Adult or Supervisor rights. Restricted accounts cannot disable any portion of Norton Internet Security. For more information, see "Logging on and logging off" on page 68.

2 In the Current Status window, select the feature that you want to disable to open its status window.

3 In the feature's status window, click **Disable**.

The feature is enabled when you click Enable or the next time you start your computer.

Keeping current with LiveUpdate

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate downloads program updates and protection updates to your computer.

Your normal Internet access fees apply when you use LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are also called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of downloading and installing program updates. It saves you the trouble of locating and downloading files from an Internet site, then installing them, and deleting the leftover files from your disk.

About protection updates

One of the most common reasons for computer virus infections is that you have not updated your protection files regularly. Symantec provides online access to protection updates by subscription.

- The virus definition service provides access to the latest virus signatures and other technology from Symantec. Norton AntiVirus, Norton SystemWorks, Norton Internet Security, and Symantec AntiVirus for Palm OS use the updates available from the virus definition service to detect the newest virus threats.
- The Web filtering service provides access to the latest lists of Web site addresses and Web site categories used to identify inappropriate Web content. Norton Internet Security uses the updates available from the Web filtering service to detect newly identified Web sites containing inappropriate content.
- The intrusion protection service provides access to the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access to your computer. Norton Personal Firewall uses the updates available from the intrusion protection service to detect the latest Internet threats.

About your subscription

Your Symantec product includes a complimentary, limited time subscription to protection updates for the subscription services used by your product. When that subscription is due to expire, you are prompted to renew your subscription. For more information, see “Subscription policy” on page 164.

If you do not renew your subscription, you can still use LiveUpdate to retrieve program updates. However, you cannot retrieve protection updates and will not be protected against newly discovered threats.

Obtain program and protection updates

Use LiveUpdate regularly to obtain protection updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

Note: If you connect to the Internet through America Online (AOL), CompuServe, or Prodigy, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.

   You might receive a warning that your subscription has expired. Follow the on-screen instructions to complete the subscription renewal.
3. Click **Next** to locate updates.
4. If updates are available, click **Next** to download and install them.
5. When the installation is complete, click **Finish**.

About Rescue Disks

Rescue Disks record a duplicate set of system startup files and disk partition information, and store rescue items and a virus scanner across multiple floppy disks or on a network drive. Rescue Disks can be made for the DOS-based Windows 98 and Windows Me operating systems; they are not needed for Windows NT, Windows 2000, or Windows XP.

A Rescue Disk set consists of one bootable floppy disk, one Norton AntiVirus Program floppy disk, and three Virus Definition floppy disks. If you have Norton Utilities installed, you will also have two Norton Utility floppy disks in your Rescue Disk set. With a Rescue Disk set, you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.

Note: Rescue Disks contain information specific to the computer on which they were made. If you are using Rescue Disks for recovery, you must use the disks made for your computer. If you are using Rescue Disks to scan for viruses, you can use disks made for a different computer. For more information, see "Using Rescue Disks in virus emergencies" on page 114.

Rescue Disks can and should be updated whenever you update your virus protection, install new software, or make changes to your hardware.

Create a Rescue Disk set

Rescue Disks can be created at any time. You start the Rescue Disk Wizard from the Norton Internet Security main window.

You will need five formatted 1.44-MB disks.

To create Rescue Disks

1. At the top of the Norton Internet Security main window, click **Rescue**.
2. Under Select Destination Drive, select drive A.
3. Click **Create**.
4. Label the five disks as specified in the Basic Rescue Disk List window and click **OK**.
5. Insert the disks as requested.

Test your Rescue Disks

At the end of the Create Rescue Disks process, you are prompted to test your disks. This requires that you restart your computer using the Rescue Disks.

To test your Rescue Disks

1. Close all open Windows programs.
2. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A, then click **Restart**.

   If the Rescue Disk screen appears on your monitor, the Rescue Disk works properly. If the Rescue Disk screen does not appear, you have several options for correcting the problem. For more information, see "My Rescue Disk does not work" on page 141.
3. Press **Escape** to exit to DOS.
4. Remove the disk from drive A, then slide open the plastic tab on the back of the disk to write-protect it.
5. Restart your computer.

Update your Rescue Disks

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

If you are updating a floppy disk set, make sure your disks are not write-protected before you begin.

To update your Rescue Disks

1. At the top of the Norton Internet Security main window, click **Rescue**.
2. Under Select Destination Drive, select drive A.
3. Click **Update**.
4. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A.
5. Click **OK**.
6. Insert the remaining disks in your set as requested.

Make sure to test your newly updated Rescue Disk set when prompted. For more information, see "Test your Rescue Disks" on page 41.

Getting help with Norton Internet Security

There are four kinds of online Help:

- Comprehensive online Help
- Detailed instructions for windows and dialog boxes
- What's This? Help for buttons and other controls
- The Readme file and Release Notes

Comprehensive online Help

The online Help contains the information in this User's Guide.

To access Online Help

1. At the top of the Norton Internet Security window, click **Help**.
2. Click **Norton Internet Security Help**.

Window and dialog box Help

Dialog box Help provides information about the Norton Internet Security program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To get help with a window or dialog box

- Do one of the following:
  - Click the **Tell Me More** link if one is available.
  - In the dialog box, click **Help**.

What's This? Help for buttons and other controls

What's This? Help provides a definition of individual components of a window or dialog box.

To access What's This? Help

- Right-click anywhere that you need help in a window or dialog box, then click **What's This?**

Readme file and Release Notes

The Readme file contains information about installation and compatibility issues. The Release Notes contain technical tips and information about product changes that occurred after this guide went to press. They are installed on your hard disk in the same location as the Norton Internet Security product files.

To read the Readme file

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Product Support** > **readme.txt**.
   - On the Windows XP taskbar, click **Start** > **More Programs** > **Norton Internet Security** > **Product Support** > **readme.txt**.

   The file opens in Notepad.
2. Close the word processing program when you are done reading the file.

The Release Notes also can be accessed from the Start menu.

To read the Release Notes

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Product Support** > **Norton Internet Security Release Notes**.
   - On the Windows XP taskbar, click **Start** > **More Programs** > **Norton Internet Security** > **Product Support** > **Norton Internet Security Release Notes**.

   The file opens in Notepad.
2. Close the word processing program when you are done reading the file.

Using the Security Assistant

The Security Assistant is always available to provide information on how Norton Internet Security works, or to change any of the settings you selected.

To use the Security Assistant

1. At the top of the Norton Internet Security window, click **Assistant**.
2. At the bottom of each pane, click **Next** to progress through the Security Assistant.
3. Click **Close** to close the Security Assistant.

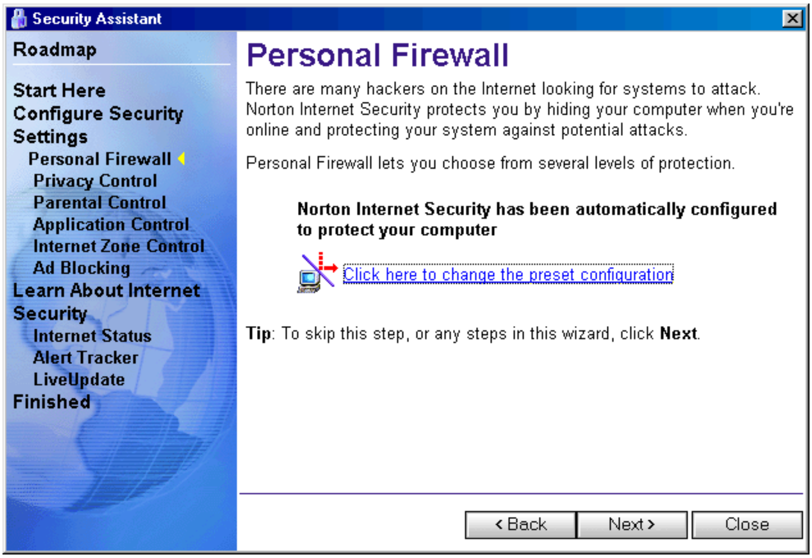
The purpose of each pane is described in the following sections.

Personal Firewall

Personal Firewall protects your computer from unauthorized access while you are connected to the Internet. You can choose to have Personal Firewall enabled or disabled. If it is enabled (the default setting), you can also choose the level of protection provided.

To enable Personal Firewall

1. In the Security Assistant Roadmap, click **Personal Firewall**.



Personal Firewall

There are many hackers on the Internet looking for systems to attack. Norton Internet Security protects you by hiding your computer when you're online and protecting your system against potential attacks.

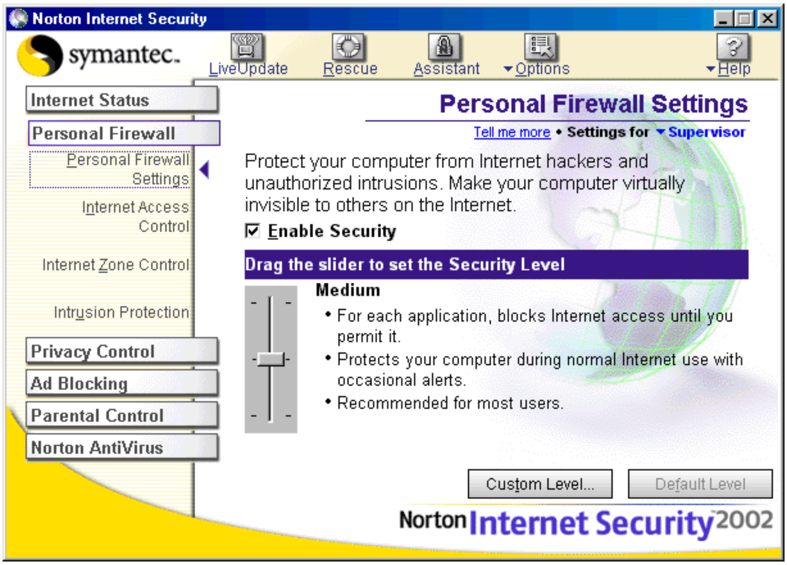
Personal Firewall lets you choose from several levels of protection.

Norton Internet Security has been automatically configured to protect your computer

Click here to change the preset configuration

Tip: To skip this step, or any steps in this wizard, click **Next**.

2 Click **Click here to change the preset configuration**.



Personal Firewall Settings

Tell me more • Settings for Supervisor

Protect your computer from Internet hackers and unauthorized intrusions. Make your computer virtually invisible to others on the Internet.

☑ Enable Security

Drag the slider to set the Security Level

Medium

- For each application, blocks Internet access until you permit it.
- Protects your computer during normal Internet use with occasional alerts.
- Recommended for most users.

3 Check **Enable Security**.

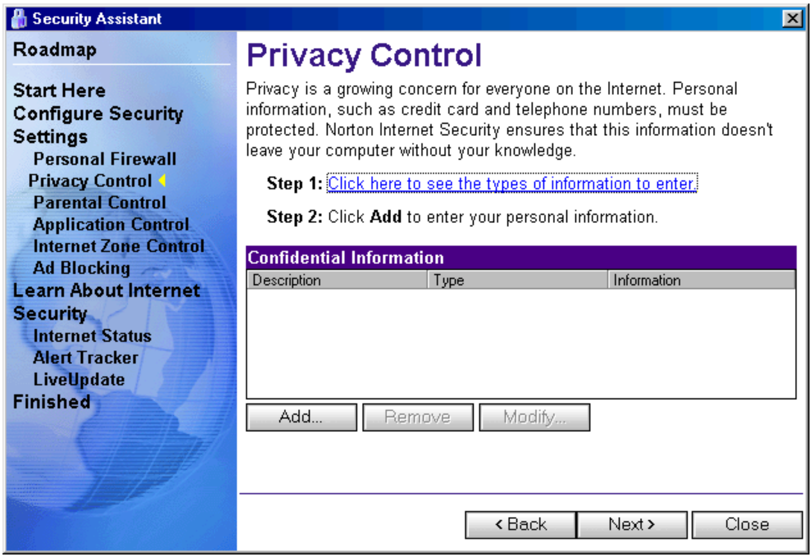
For more information, see “Setting the Security Level” on page 93.

Privacy Control

Using Privacy Control, you can identify confidential information stored on your computer that should have extra protection. Any items that you put on this list are blocked from being released to any Web site that does not use secure, encrypted communications, and they are blocked from being sent through the supported instant messenger programs.

To add confidential information to be blocked

1 In the Security Assistant Roadmap, click **Privacy Control**.



Privacy Control

Privacy is a growing concern for everyone on the Internet. Personal information, such as credit card and telephone numbers, must be protected. Norton Internet Security ensures that this information doesn't leave your computer without your knowledge.

Step 1: Click here to see the types of information to enter.

Step 2: Click **Add** to enter your personal information.

Confidential Information

Description	Type	Information

2 In the Privacy Control pane, click **Add**.

3 In the Add Confidential Information dialog box, select a category in the Type of information to protect box.

4 In the Descriptive name field, type a description to help you remember why you are protecting the data.

5 In the Information to protect field, type the information you want to block from being sent through nonsecure Internet connections.

6 Click **OK**.

For more information, see "Adding confidential information to be blocked" on page 72.

Parental Control

Parental Control allows you to control your children's access to the Internet. You can block access to categories of sites that you find inappropriate and you can block access to applications, such as chat, that you don't want your children to use on the Internet.

Internet access is defined by user account. You can use Windows accounts that you have already established, or you can create new accounts.

Creating and defining accounts can be done using the Parental Control Wizard. For more information, see “Controlling access to Web content” on page 53.

Application Control

Norton Internet Security can scan your computer for Internet-enabled applications and create access rules for them. When the scan is complete, you can use the results to determine which applications should have access to the Internet and, if desired, adjust their access rules.

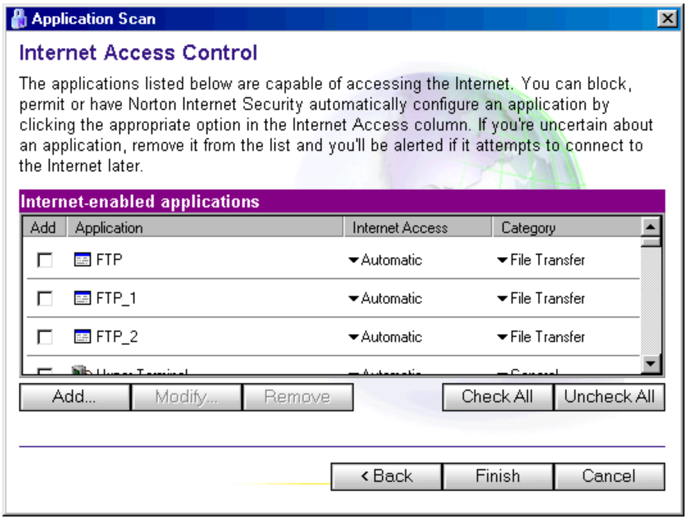
To scan for Internet-enabled applications

1 In the Security Assistant Roadmap, click **Application Control**.

2 In the Application Control pane, click **Click here to scan for Internet applications**.

3 In the Application Scan window, click **Next** to begin the scan.

When the scan is complete, all Internet-enabled applications that were found are listed.



Internet Access Control

The applications listed below are capable of accessing the Internet. You can block, permit or have Norton Internet Security automatically configure an application by clicking the appropriate option in the Internet Access column. If you're uncertain about an application, remove it from the list and you'll be alerted if it attempts to connect to the Internet later.

Internet-enabled applications

Add	Application	Internet Access	Category
□	FTP	Automatic	File Transfer
□	FTP_1	Automatic	File Transfer
□	FTP_2	Automatic	File Transfer
□	Hyper Terminal	Automatic	General

4 To allow Internet access for an application, check the box to the left of the application’s name.

5 To change the Internet access rule or category of an application, select the setting you want from the appropriate drop-down list.

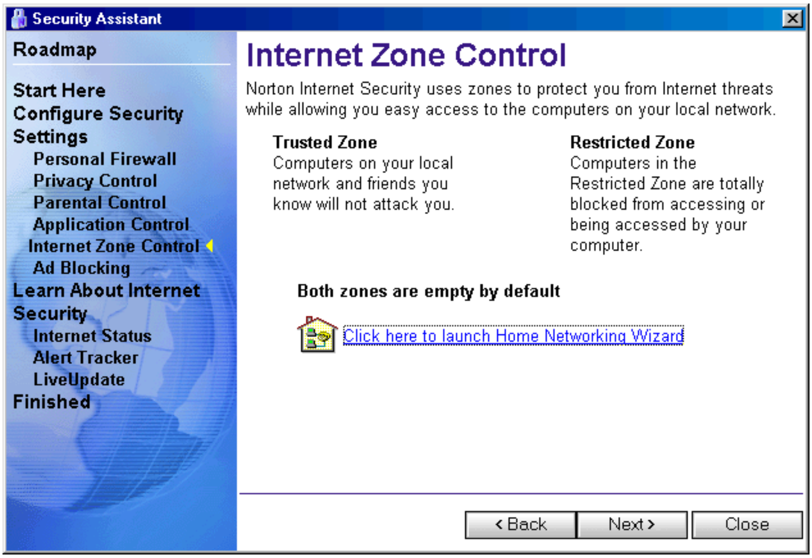
6 Click **Finish** when you are done.

Internet Zone Control

Use Internet Zone Control to identify computers to which you want to grant access to your computer and those to which you want to deny access. The Home Network Wizard can automatically configure your home network and add computers in that network to your Trusted Zone.

To run the Home Network Wizard from the Security Assistant

1 In the Security Assistant Roadmap, click **Internet Zone**.



Internet Zone Control

Norton Internet Security uses zones to protect you from Internet threats while allowing you easy access to the computers on your local network.

Trusted Zone
Computers on your local network and friends you know will not attack you.

Restricted Zone
Computers in the Restricted Zone are totally blocked from accessing or being accessed by your computer.

Both zones are empty by default

Click here to launch Home Networking Wizard

2 In the Internet Zone Control pane, click **Click here to launch Home Networking Wizard**.

3 Follow the on-screen instructions.

For more information, see “Home network control with Internet Zone Control” on page 101.

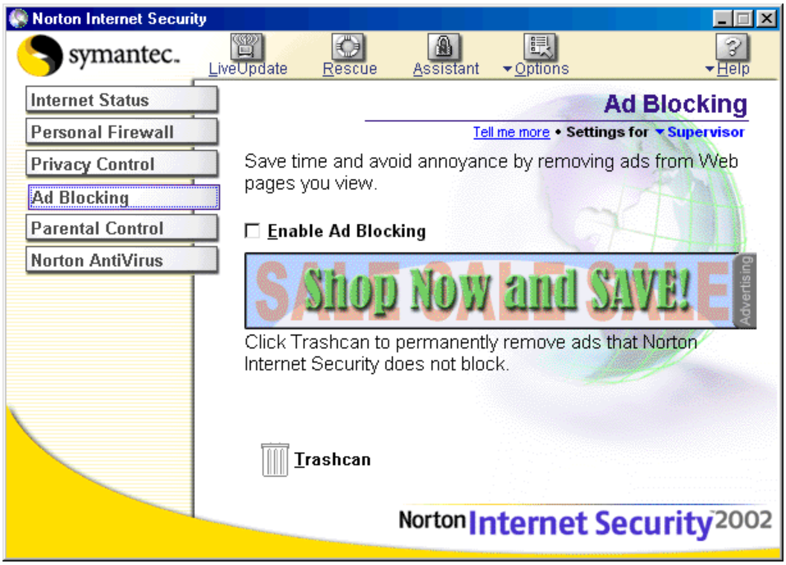
Ad Blocking

Ad Blocking blocks Internet advertisements from downloading, reducing the amount of time it takes to download a Web page.

To enable Ad Blocking

1 In the Security Assistant Roadmap, click **Ad Blocking**.

2 In the Ad Blocking pane, click **Click here to turn Ad Blocking on or off**.



Save time and avoid annoyance by removing ads from Web pages you view.

□ Enable Ad Blocking

Click Trashcan to permanently remove ads that Norton Internet Security does not block.

3 Check **Enable Ad Blocking**.

For more information, see "Blocking Internet advertisements" on page 77.

Internet Status

Norton Internet Security tracks activity that occurs on your computer while you are connected to the Internet. You can check on this activity using Internet Status.

To check Internet Status

1 In the Security Assistant Roadmap, click **Internet Status**.

2 To see the current status of your Internet activity, click **Current Status**.

For more information, see “Monitoring Norton Internet Security events” on page 119.

3 To adjust the amount of information displayed in Current Status, click **Reporting**.

For more information, see “Adjusting the reporting detail” on page 90.

Alert Tracker

The Alert Tracker appears as a half globe on the side of your screen. When an event occurs that Norton Internet Security reports on, Alert Tracker briefly displays a message to inform you. You can also use Alert Tracker to block Web page ads. For more information, see “Using Alert Tracker” on page 89.

LiveUpdate

LiveUpdate provides a way for you to receive program and protection updates. For more information, see “Keeping current with LiveUpdate” on page 37.

Running Security Check

Use Security Check to test your computer's vulnerability to security intrusions. The Security Check link in Norton Internet Security connects you to the Symantec Web site, on which you can get detailed information about what Security Check scans for, and from which you can run the scan.

To run Security Check

1. On the left side of the Norton Internet Security window, click **Internet Status > Security Check**.
2. In the Security Check window, click **Scan for Security Risks**.

   Your browser opens on the Symantec Security Check Web page.
3. To learn more about what Security Check does, in the Security Check Web page, click **About Scan for Security Risks**.
4. To run the scan, click **Scan for Security Risks**.

When the scan is complete, the results page lists all the areas checked and your level of vulnerability in each one. For any area marked as at risk, you can get more details about what the problem is and how to fix it.

To get more information about a scanned area

- In the results page, next to the scan name, click **Show Details**.

  If the area is at risk, the details include suggestions for fixing the problem.

CHAPTER 4

Controlling access to Web content

While the Internet provides opportunities to bring information into the home, it also contains information that is inappropriate for children or other family members.

The most effective way to keep these types of materials from entering your home is to talk with your family about the appropriateness of Internet content. Norton Internet Security helps you enforce the decisions your family makes about how they use the Internet.

Parental Control lets parents control which Web sites their children visit and which types of applications they use to access the Internet. This effectively blocks inappropriate Web sites and prevents the use of chat software or other applications.

Configuring Parental Control is a two part process. First, identify and set up accounts for the users, then set controls for the accounts. When a user logs on to an account, Norton Internet Security sets the appropriate restrictions until that user logs off.

Understanding accounts

Norton Internet Security uses accounts assigned to those who use your computer to control their access to the Internet. An account stores the type of Internet access allowed for the users assigned to the account.

You can use the accounts that you have set up for your Windows operating system, or you can create new ones specifically for Norton Internet Security.

The account created during installation is a Supervisor account. With a Supervisor account, you can change any of the settings in Norton Internet Security and create additional accounts.

You can create as many accounts as you need. You can customize the settings of any account to provide the exact level of protection needed for children, teenagers, and adults. If you are the only person who uses your computer, you do not need to create additional accounts.

Note: When no account is active, Norton Internet Security uses the restricted settings of Not Logged In, which shuts down all Internet access. If you are using Windows accounts, this situation does not occur.

Understanding account restrictions

Parental Control restricts access to the Internet in two ways:

- Restricts Web site access
- Restricts applications that access the Internet

Restricting Web site access

Parental Control comes with an extensive list of categorized Web sites. This list is updated regularly by Symantec. Use LiveUpdate to keep the list current.

For more information, see “Keeping current with LiveUpdate” on page 37.

You can restrict an account’s access by choosing one of the following methods:

- Use the list of categorized sites to specify which categories an account can and cannot access. You can also add your own sites to the list of blocked sites. Use this option to restrict an account from visiting specific Web sites or Web site categories, but to allow everything else.
- Create a list of Web sites that can be visited. All accounts that use this method can only browse the Web sites on this list. Use this option for young children’s accounts when you want to strictly control their Internet activities.

For more information, see “Restricting access to Web sites” on page 64.

Restricting applications that access the Internet

You can decide which types of applications that each account can use on the Internet. For example, parents can prevent children from using chat applications by blocking the chat applications category from the children's accounts. For more information, see "Blocking applications from accessing the Internet" on page 66.

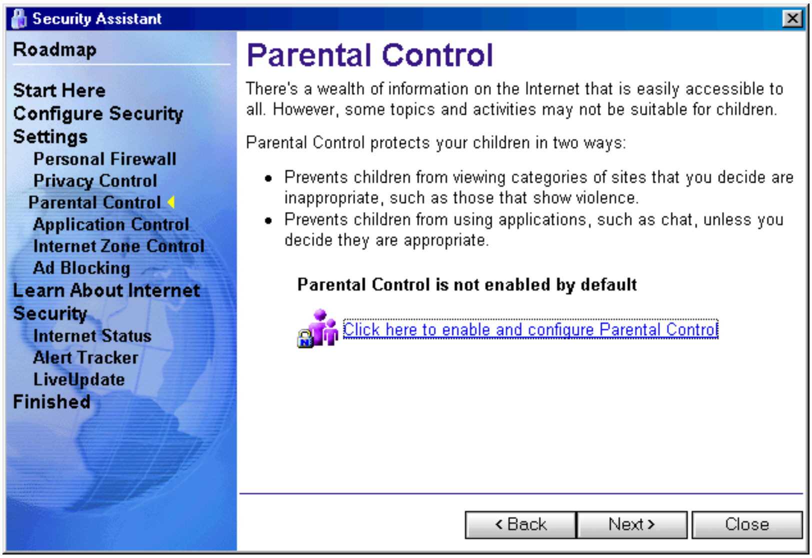
Using your Windows accounts

If you want to use your Windows accounts as Parental Control accounts, use the Parental Control Wizard.

To use your Windows accounts

1 At the top of the Norton Internet Security main window, click **Assistant**.

2 In the Security Assistant Roadmap, click **Parental Control**.



Parental Control

There's a wealth of information on the Internet that is easily accessible to all. However, some topics and activities may not be suitable for children.

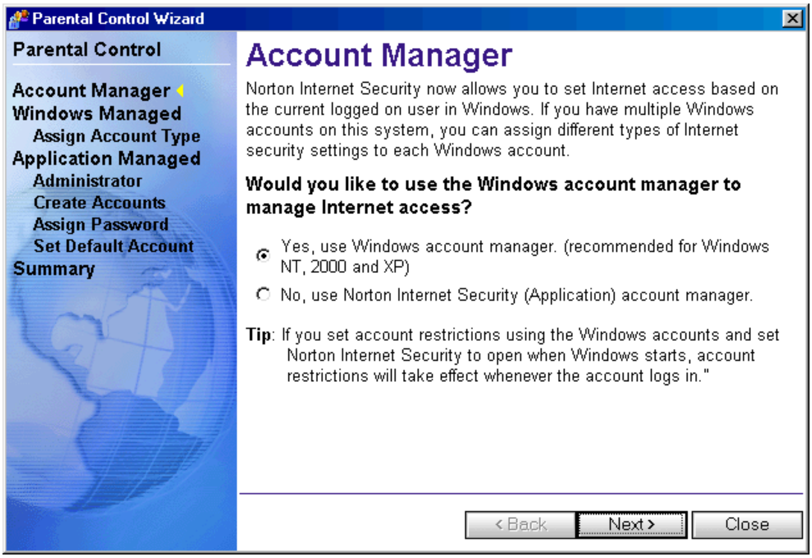
Parental Control protects your children in two ways:

- Prevents children from viewing categories of sites that you decide are inappropriate, such as those that show violence.
- Prevents children from using applications, such as chat, unless you decide they are appropriate.

Parental Control is not enabled by default

Click here to enable and configure Parental Control

3 In the Parental Control pane, click **Click here to enable and configure Parental Control**.



Account Manager

Norton Internet Security now allows you to set Internet access based on the current logged on user in Windows. If you have multiple Windows accounts on this system, you can assign different types of Internet security settings to each Windows account.

Would you like to use the Windows account manager to manage Internet access?

● Yes, use Windows account manager. (recommended for Windows NT, 2000 and XP)

○ No, use Norton Internet Security (Application) account manager.

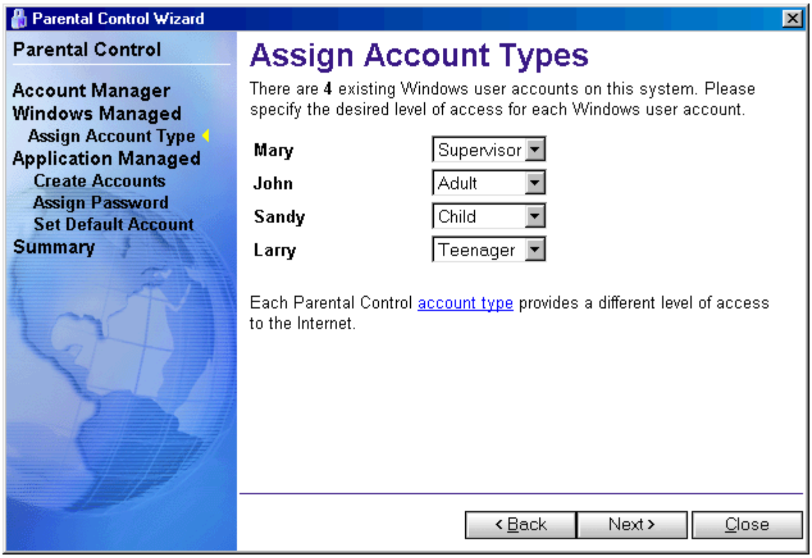
Tip: If you set account restrictions using the Windows accounts and set Norton Internet Security to open when Windows starts, account restrictions will take effect whenever the account logs in."

4 In the Account Manager pane of the Parental Control Wizard, click **Yes, use Windows account manager**.

5 Click **Next**.

In the Assign Account Types pane, all your currently defined Windows accounts are listed.

6 For each account, select an account type. For more information, see "Creating accounts with the Norton Internet Security window" on page 61.



Assign Account Types

There are **4** existing Windows user accounts on this system. Please specify the desired level of access for each Windows user account.

Mary	Supervisor
John	Adult
Sandy	Child
Larry	Teenager

Each Parental Control account type provides a different level of access to the Internet.

7 Click **Next**.

8 Click **Finish** to close the Parental Control Wizard.

9 Click **Close** to close the Security Assistant.

If you want to customize the settings for each account, use the Parental Control Settings pane in the Norton Internet Security main window. For more information, see "Setting up account restrictions" on page 63.

Setting up your own accounts

If you are setting up your own accounts, you can establish family accounts that all members of your family requiring the same level of access or restriction can use. You can use either the Parental Control Wizard or the Norton Internet Security main window to create the accounts.

About family accounts

Parental Control helps you enforce the decisions that your family makes about how they use the Internet. You can create separate accounts for people or groups of people with different Internet use needs.

Only adults use the computer

If you are the only user, you do not need any additional accounts. The Supervisor account created during installation is the startup account, with Supervisor rights, and is active whenever you use Norton Internet Security.

If more than one adult uses the computer, you can create separate accounts or they can share a single account.

If the other adults want to change their own settings, create separate accounts for each of them. If they need to create accounts or change settings for other accounts, they must use a Supervisor account.

For more information, see "Managing accounts" on page 60.

Adults and children use the computer

Norton Internet Security gives you control over the Web sites that children can visit. You can set up Norton Internet Security so that whenever the computer is started, the children's settings take effect. Then, when you want to use the computer, you can log on to Norton Internet Security under a less restrictive account.

If you have several children with similar needs and want them all to use the same security settings, they can share the same account.

If you want to give different access privileges to different groups of children, you must use separate accounts for each group.

To ensure that younger children cannot access the Internet using the older children's account, make sure that the older children log off when they are finished.

Creating accounts with the Parental Control Wizard

You can use the Parental Control Wizard to create accounts and assign account types.

To create accounts with the Parental Control Wizard

1. At the top of the Norton Internet Security main window, click **Assistant**.
2. In the Security Assistant Roadmap, click **Parental Control**.
3. In the Parental Control pane, click **Click here to enable and configure Parental Control**.
4. In the Account Manager pane of the Parental Control Wizard, click **No, use Norton Internet Security (Application) account manager**.
5. Click **Next**.
6. In the Create Additional Accounts pane, type an account name and choose an account type for each account you want to create.
7. Click **Next**.
8. If the account displayed requires a password, type it in the Password and Confirm Password fields.
9. Click **Next**.
10. If you added multiple accounts, the Password Page appears for each one. Repeat steps 9 and 10 for all accounts added.
11. Choose a default account to be used by Norton Internet Security when no one is logged on to Norton Internet Security.
12. Click **Next**.
13. Click **Finish** to close the Parental Control Wizard.
14. Click **Close** to close the Security Assistant.

Enabling Parental Control

Enable Parental Control for those accounts you want to restrict.

To enable Parental Control

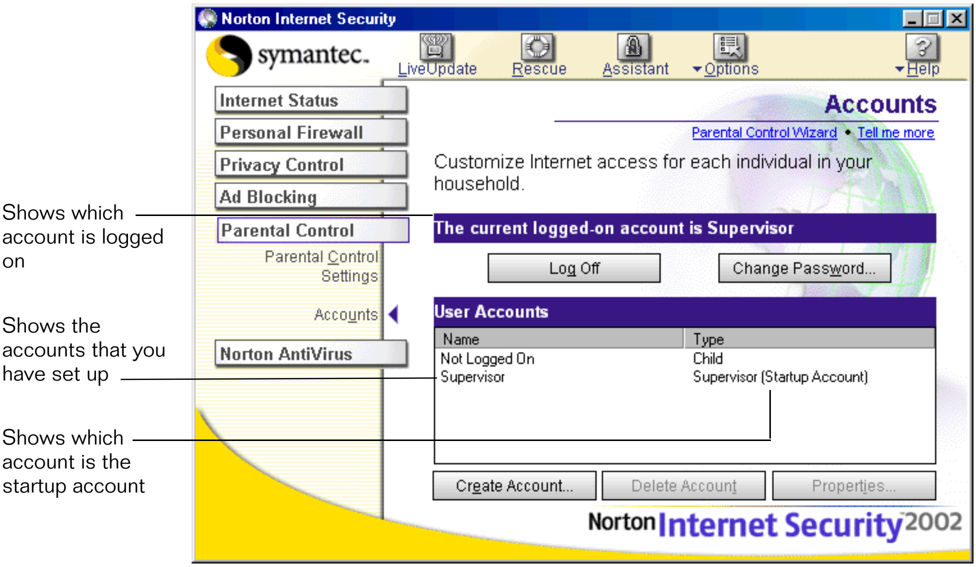
1. On the left side of the Norton Internet Security window, click **Parental Control** > **Parental Control Settings**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Check **Enable Parental Control**.

Managing accounts

Norton Internet Security accounts control users' access to the Internet. Managing accounts includes:

- Creating new accounts
- Changing account settings
- Choosing the startup account

The Accounts window allows a user logged on to a Supervisor account to create and manage accounts.



Customize Internet access for each individual in your household.

The current logged-on account is Supervisor

Name	Type
Not Logged On	Child
Supervisor	Supervisor (Startup Account)

Shows which account is logged on

Shows the accounts that you have set up

Shows which account is the startup account

Creating accounts with the Norton Internet Security window

When you create an account, you assign an account type. The account type sets appropriate settings throughout Norton Internet Security.

Account Type	Description
Child	Turns on Parental Control, blocking most Web sites and applications that connect to the Internet.
Teenager	Turns on Parental Control and blocks some Web sites and Internet-enabled applications.
Adult	Turns off Parental Control. Normal account users can change their own security settings.
Supervisor	Turns off Parental Control. Supervisors can change settings for any account.

Only Supervisor accounts can create additional accounts.

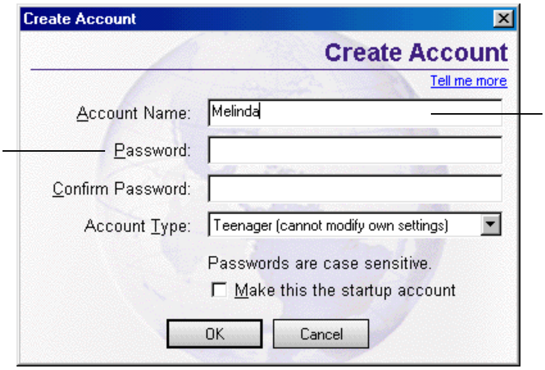
To create a user account

1 Log on to Norton Internet Security with an account that has Supervisor rights.

For more information, see "Logging on and logging off" on page 68.

2 On the left side of the Norton Internet Security window, click **Parental Control** > **Accounts**.

3 Click **Create Account**.



Account Name: Melinda

Password:

Confirm Password:

Account Type: Teenager (cannot modify own settings)

Passwords are case sensitive.

□ Make this the startup account

Protecting the account with a password helps prevent others from using the account

Give the account a name that describes how the account will be used

4 In the Create Account window, type the name of the new account.

5 In the Password field, type a password if needed.

If you are creating an account that you do not want others to use, password protect it. Passwords might not be necessary for young children's accounts or startup accounts.

6 If you entered a password, in the Confirm Password field, type it again.

7 In the Account Type field, select an account type.

The account type sets appropriate settings throughout Norton Internet Security.

Changing settings for a Supervisor account

You can change the settings for a Supervisor account while you are logged on to an account with Supervisor rights.

To change settings for a Supervisor account

1 Log on to Norton Internet Security with an account that has Supervisor rights.

For more information, see "Logging on and logging off" on page 68.

2 Go through the settings for Security, Privacy, Ad Blocking, and Parental Control to personalize Norton Internet Security.

Changing settings for normal and restricted accounts

You can change settings for any account while you are logged on to an account with Supervisor rights.

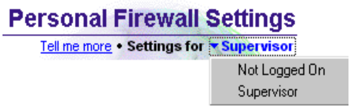
To change settings for normal and restricted accounts

1 Log on to Norton Internet Security with an account that has Supervisor rights.

For more information, see "Logging on and logging off" on page 68.

2 On the left side of the Norton Internet Security window, select the window in which you want to make changes.

3 Click the **Settings For** arrow and select the account that you want to change.


Personal Firewall Settings
Tell me more • Settings for Supervisor
Not Logged On
Supervisor

The settings for the selected account appear in the current window.

4 Change the settings for that account.

Setting the startup account

Each time Norton Internet Security starts, one of the user accounts is automatically logged on. This account, known as the Startup Account, provides the initial configuration settings for Norton Internet Security.

The startup account should be the account with the most restrictions. This ensures that everyone uses the most protected settings unless they know how to open Norton Internet Security and change to a different account.

To set an account as the startup account

1 On the left side of the Norton Internet Security window, click **Parental Control** > **Accounts**.

2 Select the user account that you want to make the startup account.

3 Click **Properties**.

4 In the Account Properties dialog box, check **Make this the startup account**.

Setting up account restrictions

When you are logged on to a Supervisor account, you can use Parental Control to set the Internet access permissions for your children.

To set up account restrictions

1 On the left side of the Norton Internet Security window, click **Parental Control** > **Parental Control Settings**.

2 Click the **Settings For** arrow and select the account that you want to change.

3 Ensure that Enable Parental Control is checked.

4 Restrict access to Web sites.

For more information, see “Restricting access to Web sites” on page 64.

5 Block applications from accessing the Internet.

For more information, see “Blocking applications from accessing the Internet” on page 66.

Restricting access to Web sites

You can specify categories of Web sites that an account can or cannot visit.

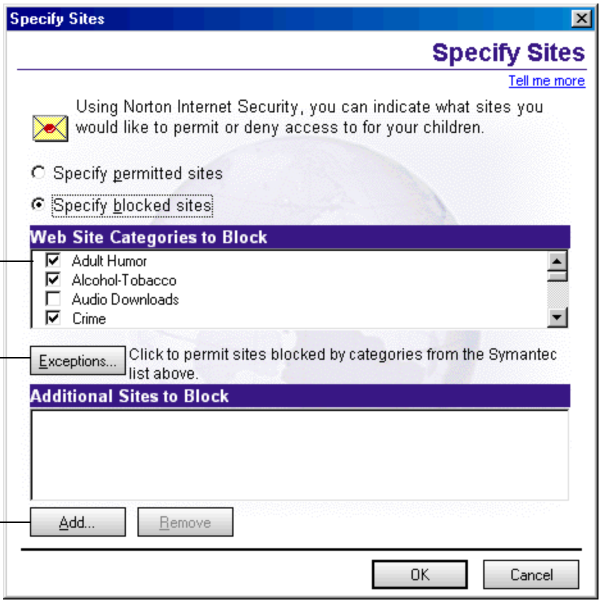
To block Web site categories

1 On the left side of the Norton Internet Security window, click **Parental Control > Parental Control Settings**.

2 Click the **Settings For** arrow and select the account that you want to change.

3 Click **Sites**.

4 In the Specify Sites window, click **Specify Blocked Sites**.



Specify Sites

Specify Sites

Tell me more

Using Norton Internet Security, you can indicate what sites you would like to permit or deny access to for your children.

○ Specify permitted sites

● Specify blocked sites

Web Site Categories to Block

☑ Adult Humor
☑ Alcohol-Tobacco
☐ Audio Downloads
☑ Crime

Exceptions... Click to permit sites blocked by categories from the Symantec list above.

Additional Sites to Block

This account can’t visit Web sites in checked categories

Create an exception to unblock a site without disabling the entire category

Add additional Web sites that you want to block

5 Under Web Site Categories to Block, check the categories that you want to block for this account.

Use LiveUpdate to keep the list of categorized Web sites up-to-date.

For more information, see "Keeping current with LiveUpdate" on page 37.

Creating a list of permitted Web sites

Instead of blocking categories of Web sites, you can create a list of permitted Web sites. Any sites not on the list of permitted Web sites are blocked.

To create a list of permitted Web sites

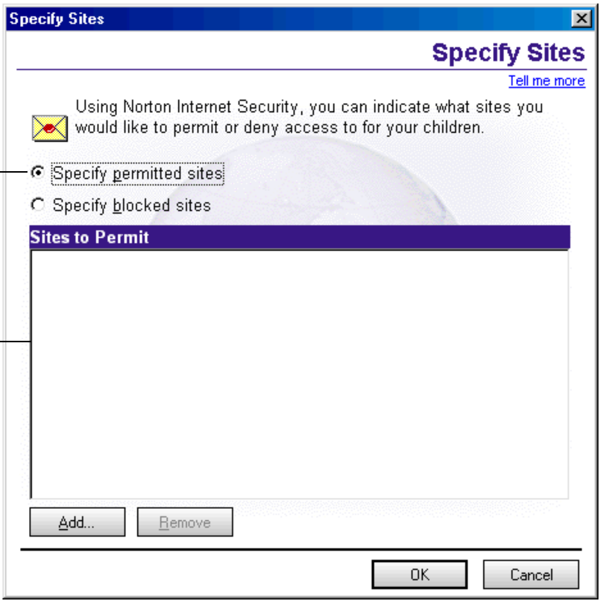
1 On the left side of the Norton Internet Security window, click **Parental Control > Parental Control Settings**.

2 Ensure that Enable Parental Control is checked.

3 Click the **Settings For** arrow and select the account that you want to change.

4 Click **Sites**.

5 In the Specify Sites window, click **Specify Permitted Sites**.



Using Norton Internet Security, you can indicate what sites you would like to permit or deny access to for your children.

● Specify permitted sites
○ Specify blocked sites

Sites to Permit

This account can visit only the sites listed in this window

Add Web sites to the list

6 Click **Add** to create a new entry in the list.

7 In the Add Web site To Permitted List window, type the complete address of the Web site.

The Sites To Permit list is the same for all accounts that use it. You cannot create a separate list of permitted Web sites for different accounts.

Submitting Web sites to Symantec

You can help improve the Norton Internet Security list of Web sites for Parental Control. For example, you might find a Web site that should be added to the list. Perhaps a Web site is being blocked under one category, and you think it belongs under other categories as well. Maybe you have a Web site that you think should be removed from the list.

To submit suggested changes to the Norton Internet Security list, visit http://www.symantec.com/avcenter/cgi-bin/nisurl.cgi

Blocking applications from accessing the Internet

Parental Control blocks categories of applications from accessing the Internet. You can use these categories to control the applications that your children use.

Norton Internet Security defines the following categories.

Category	Explanation
General	Applications that do not fall under any other category can be placed in this category.
Chat	Applications that let you engage in conversations with other users or communities online using text, voice, or video. Examples include mIRC, Pirch, ICQ, NetMeeting, Internet Phone, Net2Phone, and CU-SeeMe. Restricting this category of applications does not block Web-based chat that appears in your browser.
Conferencing & Collaboration	Applications that let two or more users communicate directly with one another. This category includes applications that let users collaborate through the use of an application, such as whiteboard applications and Web browsers. Examples include NetMeeting, ICQ, Microsoft Instant Messenger, Yahoo! Messenger, and Internet Phone.

Category	Explanation
Email	Applications that access email servers, known as email clients. Examples include Microsoft Outlook Express and Eudora. Restricting this category of applications does not block Web-based email that appears in your browser, such as HotMail.
Education & Family	Educational applications that are appropriate for children and that access the Internet.
File Transfer	Applications that let users transfer files to and from their computers. Examples include CuteFTP and BulletFTP.
Instant Messaging	Applications that are similar to chat applications, but are designed to run in the background to allow users instant access to a user who is currently running the same instant messenger client. Examples include ICQ, Yahoo! Messenger, Microsoft Instant Messenger, AOL Instant Messenger, and TribalVoice.
Newsreaders	Applications that access newsgroups.
Networked Games	Games that access a network or the Internet to let users play with or against one another.
Web Browsers	Applications that provide users with access to the World Wide Web. Examples include Microsoft Internet Explorer and Netscape Navigator.
User Categories	Additional categories that you can use to create other classifications of applications.

The Personal Firewall must be set to High for application restrictions to work. The Personal Firewall is set to High when the Personal Firewall Settings Security Level is set to Medium or High.

For more information, see “Setting the Security Level” on page 93.

For more information, see “Changing the Personal Firewall setting” on page 95.

To set up application categories for an account

1. On the left side of the Norton Internet Security window, click **Parental Control > Parental Control Settings**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Click **Applications**.
4. In the Applications dialog box, select the categories that this account is allowed to use.

Note: Blocking an application does not prevent the user from opening or running the application. It only prevents the application from making a connection with the Internet. Because of this, the application may freeze or crash when Norton Internet Security prevents it from connecting to the Internet. It may not be obvious what causes the problem.

Logging on and logging off

When you start Norton Internet Security, it uses the settings from the startup account, or, if you are using Windows accounts, the settings for the account you use to log on to Windows. To use a different account, you have to log off of the current account and log on to another account.

Finding out which account you are currently using

If you are not sure which account is active, you can check the active account.

To find out which account is active

1. On the left side of the Norton Internet Security window, click **Internet Status > Current Status**.
2. In the upper-right corner, read the Logged on account.

Logging on to another account

You can change from one account to another by logging off and logging on.

To log on to another account

1. On the left side of the Norton Internet Security window, click **Parental Control** > **Accounts**.
2. If you are currently logged on, click **Log Off**.
3. Click **Log On**.
4. In the Log On dialog box, select the account you want to use.
5. Type the password if required.

As soon as you change the account, Norton Internet Security begins using the settings associated with that account. The Accounts window shows which account is currently active.

You can also log on and log off by clicking the Norton Internet Security icon in the notification area at the far end of the Windows taskbar, and choosing the appropriate command from the menu.

Logging off

When you log off, the settings for Not Logged In become active. To turn off protection, disable Norton Internet Security or set Norton Internet Security so that it does not start when you start your computer.

For more information, see "Temporarily disabling Norton Internet Security" on page 36.

To log off of Norton Internet Security

1. On the left side of the Norton Internet Security window, click **Parental Control** > **Accounts**.
2. Click **Log Off**.

CHAPTER 5

Protecting confidential information

Computers and Web sites collect personal information as you browse the Internet. A computer's security features might not always protect your personal information. Privacy Control helps protect your privacy by preventing these types of intrusions.

Privacy Control ensures that you don't send private information such as credit card numbers over the Internet unless they are encrypted, or you specifically allow it.

Web sites use *cookies* to track your Internet usage. While most sites use cookies to remember the choices you have made on that site, some sites use cookies to track your browsing habits. Norton Internet Security has several levels of control over cookies.

Your browser might provide more information than you like to the Web sites you visit. For example, most browsers give Web sites the address of the site you last visited. Privacy Control stops your browser from sending this type of information.

Setting the Privacy Level

The Privacy Level slider lets you select minimal, medium, or high privacy settings.

Setting	Description
High	All personal information is blocked from the Internet. An alert appears each time a cookie is encountered.
Medium (recommended)	An alert appears if confidential information is entered on a Web form or in an instant messenger. Conceals your browsing from Web sites. Cookies are not blocked.
Minimal	Confidential information is not blocked. Cookies are not blocked. Conceals your browsing from Web sites.

To set the Privacy Level

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Move the **Privacy Level** slider to the Privacy Level you want.

Adding confidential information to be blocked

There are many Web sites that ask for personal information that can jeopardize your privacy or let others steal from you. Also, any information sent using an instant messenger program is nonsecure.

If you are using Norton Internet Security accounts, there might be an account that you want to restrict from entering personal information on a nonsecure Web site. You can also restrict the account from using secure Web sites to ensure more privacy.

For more information, see “Enabling secure Web connections” on page 75.

Norton Internet Security lets you create a list of personal information that is censored from all nonsecure Internet communications.

To add confidential information to be blocked

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click **Confidential Info**.
3. In the Confidential Information dialog box, click **Add**.
4. In the Add Confidential Information dialog box, select a category in the Type Of Information To Protect box.
5. In the Descriptive Name field, type a description to help you remember why you are protecting the data.
6. In the Information To Protect field, type the information you want to block from being sent through nonsecure Internet connections.

Note: When you add confidential information to this list, the information applies to all user accounts. Any account that is blocking confidential information blocks the same list of information.

Tips on entering confidential information

Because Norton Internet Security blocks personal information exactly the way that you enter it into the program, it is better to enter only partial numbers. For example, a phone number could be typed as 888-555-1234, but it could also be entered without dashes (8885551234) or with spaces (888 555 1234), or even in two or more separate boxes. One common aspect of these formats is that the last four digits (1234) are always together. Thus, you can have better protection by protecting the last four digits than you have by protecting the entire number.

Entering partial information has two advantages. First, you are not entering your complete credit card number where someone might find it. Second, it lets Norton Internet Security block your private information on sites that use multiple boxes for credit card numbers.

Adjusting privacy settings

You can change the settings for Confidential Information, Cookie Blocking, Browser privacy, and Secure Connections if the Privacy Level settings do not meet your needs.

Changing the Confidential Information setting

Confidential Information has three settings:

- High: Blocks all confidential information.
- Medium: Alerts you each time that you attempt to send confidential information to a nonsecure Web site or through an instant messenger.
- None: Does not block confidential information.

To change the Confidential Information setting

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Click **Custom Level**.
4. Select the Confidential Information setting that you want.

Changing the Cookie Blocking setting

Cookies are small files that your browser saves on your computer. Sometimes Web sites use them for information that makes it more convenient for you to use their sites.

Cookies that record personal information can jeopardize your privacy by letting others access them without your permission. They might contain enough information to show your browsing habits, or they could expose passwords and logon names.

When a Web site requests a cookie from your computer, Norton Internet Security checks to see whether you are permitting cookies, blocking cookies, or using Cookie Alerts to determine the action.

Cookie Blocking has three settings:

- High: Blocks all cookies.
- Medium: Alerts you each time a cookie is encountered.
- None: Allows cookies.

To change the Cookie Blocking setting

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Click **Custom Level**.
4. Select the Cookie Blocking setting that you want.

Enabling Browser Privacy

Browser Privacy prevents Web sites from retrieving the type of browser that you are using and finding out which Web site you last visited.

To enable Browser Privacy

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Click **Custom Level**.
4. In the Customize Privacy Settings dialog box, check **Enable Browser Privacy**.

Enabling secure Web connections

When you visit a secure Web site, your browser sets up an encrypted connection with the Web site. Information given over secure connections cannot be detected by a firewall because the information is encrypted. *Encryption* means that the information is encoded with a mathematical formula, scrambling the data into an unreadable format.

To enable secure Web connections

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Click **Custom Level**.
4. In the Customize Privacy Settings dialog box, check **Enable Secure Connections (https)**.

Blocking secure Web connections

By default, Norton Internet Security lets any account use secure connections. However, if you want to ensure that restricted accounts are not giving out confidential information to secure Web sites, you can block them from making secure Web connections. For example, parents might want to prevent children from making online purchases.

To ensure that confidential information is not sent over secure Web connections, block all secure Web connections.

To block secure Web connections

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Click **Custom Level**.
4. In the Customize Privacy Settings dialog box, uncheck **Enable Secure Connections (https)**.

CHAPTER 6

Blocking Internet advertisements

Ad Blocking blocks Internet advertisements and common graphics from downloading. Using this feature reduces the amount of time it takes to download a Web page.

Note: Ad Blocking applies only to banner ads within a Web page. Ads built into the Web interface cannot be blocked.

Norton Internet Security searches for the address of the ads being blocked as the Web page is downloaded by your browser. If it finds any addresses that match the list of ads to block, it removes the ad so that it does not appear in your browser. It leaves the rest of the Web page intact so that you can view the page without the advertisements.

To enable Ad Blocking

1. On the left side of the Norton Internet Security window, click **Ad Blocking**.
2. Click the **Settings For** arrow and select the account that you want to change.
3. Check **Enable Ad Blocking**.

Blocking specific ads

When Ad Blocking is enabled and you connect to a Web site, Norton Internet Security uses two lists to scan the Web pages as they download:

- A default list of ads that Norton Internet Security blocks automatically. Use LiveUpdate to keep the list of blocked ads current.

  For more information, see "Keeping current with LiveUpdate" on page 37.
- An ad blocking list that you create as you block specific ads. You can add to and change this list.

To block specific ads

1. On the left side of the Norton Internet Security window, click **Ad Blocking**.
2. Ensure that Enable Ad Blocking is checked.
3. Click **Trashcan**.

   The Ad Trashcan appears.
4. Open the Web page containing the advertisement that you want to block.
5. With the windows arranged so that you can see both the advertisement and the Ad Trashcan dialog box, do one of the following:
   - If you are using Microsoft Internet Explorer, drag the unwanted ad from the Web site to the Ad Blocking dialog box.
   - If you are using Netscape, right-click the advertisement and click **Copy Image Location**, then, in the Ad Trashcan, click **Paste**.

   The address for the advertisement appears in the Ad Details line of the Ad Trashcan dialog box.
6. Do one of the following:
   - Click **Add** to begin blocking this address.
   - Click **Modify** to change the entry before adding it to the ad blocking list.

   For example, if the advertisement address is http://www.advertise.org/annoying/ads/numberone.gif, you could change it to http://www.advertise.org/annoying/ads to block everything in the ads directory.

Blocking specific ads in Internet Explorer

With Internet Explorer you can use drag and drop to quickly block unwanted ads.

To block specific ads in Internet Explorer

1. Drag the ad from Internet Explorer to the Alert Tracker half globe. Do not release the mouse button.

   The Alert Tracker expands to display the Ad Trashcan.

2. Drop the ad on the Ad Trashcan.

Blocking specific ads in Netscape

With Netscape, you can quickly block specific ads.

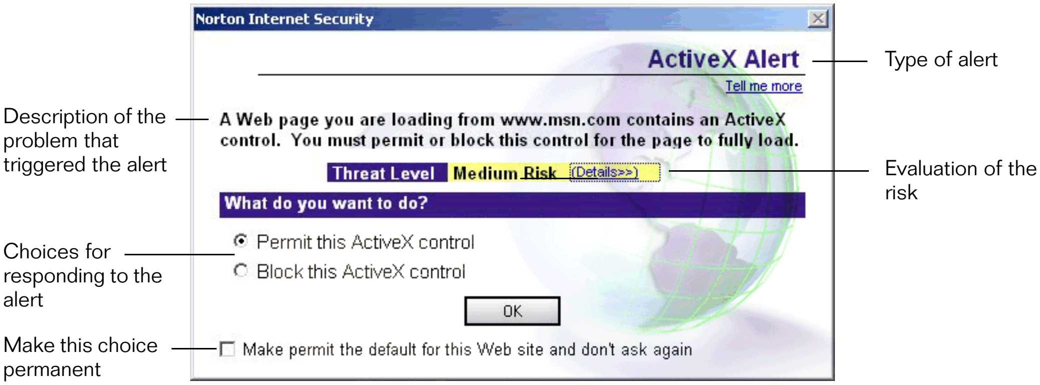
To block specific ads in Netscape

1. Right-click the ad in Netscape and click **Copy Image Location**.
2. Right-click the Alert Tracker half globe and select **Paste Ad to Trashcan**.

CHAPTER 7

Responding to Norton Internet Security alerts

Norton Internet Security monitors communication activities to and from your computer and lets you know when an activity is taking place that may compromise your security.



Norton Internet Security

ActiveX Alert

Tell me more

A Web page you are loading from www.msn.com contains an ActiveX control. You must permit or block this control for the page to fully load.

Threat Level | Medium Risk (Details>>)

What do you want to do?

● Permit this ActiveX control

○ Block this ActiveX control

OK

□ Make permit the default for this Web site and don't ask again

Type of alert

Description of the problem that triggered the alert

Evaluation of the risk

Choices for responding to the alert

Make this choice permanent

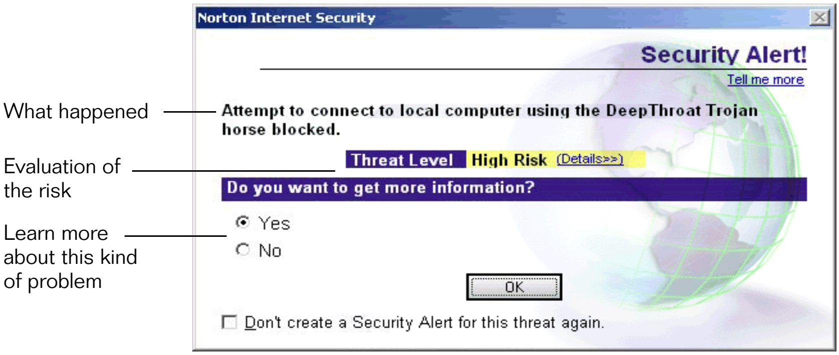
When an alert appears, read it before you make a decision. Identify what type of alert it is and the threat level. Once you understand the risks, you can make a choice.

Norton Internet Security shows the following types of alerts:

- Security Alerts
- Internet Access Control alerts
- ActiveX Alerts
- Java Alerts
- Cookie Alerts
- Confidential Information Alerts

Responding to Security Alerts

Security Alerts appear when someone attempts to access your computer. It may be a hacker or someone on your own network.



Attempt to connect to local computer using the DeepThroat Trojan horse blocked.

Do you want to get more information?

● Yes
○ No

□ Don't create a Security Alert for this threat again.

Most Security Alerts trigger AutoBlock, which prevents the computer that is attempting to connect to your computer from communicating with your computer for 30 minutes. This prevents attackers from repeatedly trying different attacks in an attempt to access your computer.

For more information, see "Using Intrusion Protection to stop attacks" on page 104.

Ensure that the alert describes a real attack and not a legitimate attempt to access your computer. If the attempt is legitimate, use Internet Access Control to allow the type of connection described in the alert.

For more information, see "Adding computers to zones" on page 101.

For more information, see "Adding an application to Internet Access Control" on page 100.

Don’t assume that every Security Alert represents an attempt to hack into your computer. There are many more-or-less harmless events on the Internet that cause Security Alerts. Answer the following questions to determine if a Security Alert represents an actual attack or normal Internet activity:

- Is the connection attempt from an unknown computer?
- Does the Security Alert describe a clearly threatening behavior? Accessing a single closed port is not as threatening as a complete port scan.
- Is the attempt part of a pattern of threatening attempts from the same computer?

If you can’t answer yes to all of these questions, you are probably not under attack. However, you might be seeing a hacker’s scan of a number of computers looking for vulnerabilities. With Norton Internet Security enabled, your computer does not appear vulnerable to the hacker. In fact, your computer may not appear to exist to the hacker at all.

For more information, see “Understanding Internet risks” on page 151.

To respond to a Security Alert

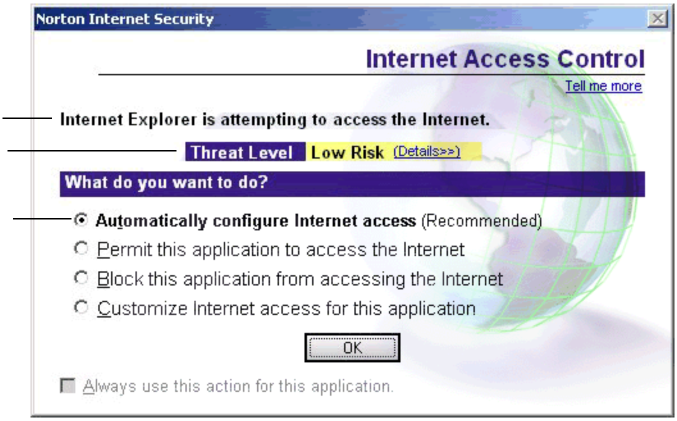
1. In the Security Alert window, click **Details** to read the information about this event.
2. Click **Yes** to learn more about this type of event.
3. If you decide that Norton Internet Security is blocking a legitimate activity, make the appropriate changes to your firewall protection or reporting.

   For more information, see “Customizing firewall protection” on page 93.

   For more information, see “Adjusting the reporting detail” on page 90.
4. Click **OK** to clear the event.

Responding to Internet Access Control alerts

Internet Access Control alerts appear when Norton Internet Security needs you to make a decision about an application on your computer that is attempting to access the Internet.



Internet Explorer is attempting to access the Internet.

Threat Level Low Risk (Details>>)

What do you want to do?

● Automatically configure Internet access (Recommended)
○ Permit this application to access the Internet
○ Block this application from accessing the Internet
○ Customize Internet access for this application

□ Always use this action for this application.

What happened

Evaluation of the risk

Select Automatic if it is available: the application is recognized and appropriate rules are created

You can minimize the number of Internet Access Control alerts by doing an Application Scan, or by enabling Automatic Internet Access Control. When this option is enabled, Norton Internet Security creates rules for applications that it recognizes without interrupting your work.

For more information, see “Scanning for Internet-enabled applications” on page 98.

For more information, see “Enabling Automatic Internet Access Control” on page 99.

To respond to an Internet Access Control alert

1. In the Internet Access Control alert window, click **Details** to read the information about this event.
2. Do one of the following:
   - Click **Automatically configure Internet access** when it is available.

     Norton Internet Security recognizes the application and has appropriate access rules in its database. This is almost always the best option to select.
   - Click **Permit this application to access the Internet** to provide the application with full access to the Internet.

     This is not as safe as choosing Automatic, but it is appropriate for many applications that Norton Internet Security does not recognize. If you recognize the application and trust that it is safe, then this is the appropriate choice.
   - Click **Block this application from accessing the Internet** to block all Internet access for the application.

     This is the appropriate choice if you don't recognize the application and the risk is high.
   - Click **Customize Internet access for this application** to create specific rules for the application's Internet access.

     Select this option if you understand how the application accesses the Internet and you want to create specific rules to control its access. Choosing this option starts the Add Rule Wizard.

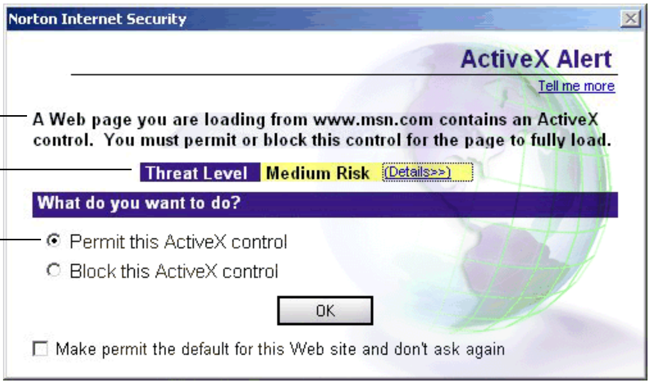
Responding to Java and ActiveX Alerts

Java applets and ActiveX controls are Web page components that do more than show text or graphics. Common applications of these components are pop-up menus and up-to-date stock quotes.

ActiveX and Java Alerts appear when you have the Security Level set to High, or have Java Applet Security or ActiveX Control Security set to Medium and a Java applet or ActiveX control is encountered.

For more information, see "Setting the Security Level" on page 93.

For more information, see "Setting Java and ActiveX Security Levels" on page 95.



A Web page you are loading from www.msn.com contains an ActiveX control. You must permit or block this control for the page to fully load.

Threat Level: Medium Risk

What do you want to do?

● Permit this ActiveX control
○ Block this ActiveX control

□ Make permit the default for this Web site and don't ask again

What happened

Evaluation of the risk

Select Permit unless the Threat Level is high or you don't trust the source

To respond to a Java or ActiveX Alert

1 In the Java or ActiveX Alert window, Click **Details** to read the information about this event.

2 Do one of the following:

- Click **Permit this ActiveX control (or Java applet)** to permit the ActiveX control or Java applet to run if you trust the integrity of the Web site.
- Click **Block this ActiveX control (or Java applet)** to prevent the ActiveX control or Java applet from running.

  While this is always the safer option, it might prevent the Web page from appearing or functioning correctly. If you select block, and the Web page does not appear or function correctly, click your browser's Refresh button and choose Permit.

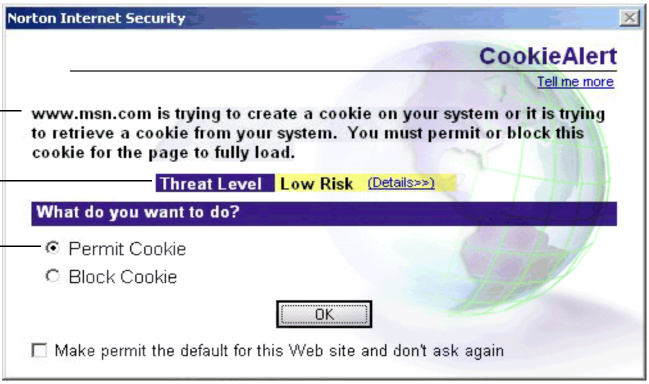
Responding to Cookie Alerts

Cookies are small files stored on your computer that Web sites use to track your visits.

Cookie Alerts appear when you have the Privacy Level set to High or Cookie Blocking set to Medium and you encounter a cookie.

For more information, see "Setting the Privacy Level" on page 72.

For more information, see “Changing the Cookie Blocking setting” on page 74.



www.msn.com is trying to create a cookie on your system or it is trying to retrieve a cookie from your system. You must permit or block this cookie for the page to fully load.

Threat Level Low Risk (Details>>)

What do you want to do?

● Permit Cookie

○ Block Cookie

□ Make permit the default for this Web site and don't ask again

What happened

Evaluation of the risk

Select Permit Cookie unless the cookie is from a site other than the one you are visiting

Because cookies are used so often and present a small security risk, you should not block cookies. However, cookies do present a significant risk to your privacy.

For more information, see “Understanding Internet risks” on page 151.

To block all cookies, and not see Cookie Alerts, change Cookie Blocking to High: Block Cookies.

To respond to a Cookie Alert

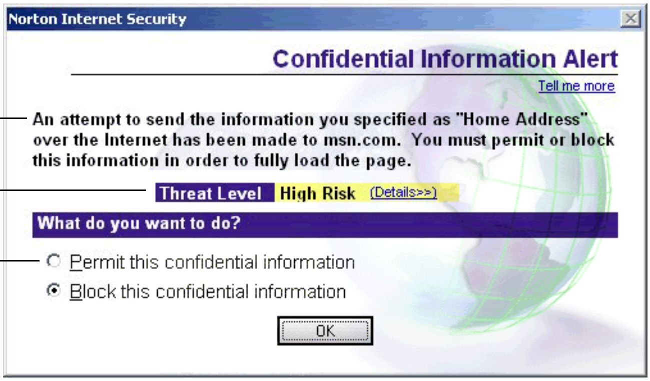
1. In the Cookie Alert window, click **Details** to read the information about this event.
2. Do one of the following:
   - Click **Permit this cookie** to allow the creation or access of the cookie.

     Cookies from the Web site that you are visiting are usually harmless and may be necessary for the Web pages to function.
   - Click **Block this cookie** to block the creation or access of the cookie.

     Expect repeated Cookie Alerts from pages on which you block cookies. Cookies that are from Web sites other than the one that you are visiting are commonly used to track your Internet usage, and can usually be blocked without affecting the operation of the Web site that you are visiting.

Responding to Confidential Information Alerts

Confidential Information Alerts appear when you attempt to send protected information to a Web site that does not use secure, encrypted communications, or when you send protected information using an instant messenger program.



Norton Internet Security

Confidential Information Alert

An attempt to send the information you specified as "Home Address" over the Internet has been made to msn.com. You must permit or block this information in order to fully load the page.

Threat Level High Risk

What do you want to do?

○ Permit this confidential information

● Block this confidential information

What happened

Evaluation of the risk

Select Permit this confidential information to allow this information to be sent

The alert includes the information that you attempted to send and to where it is being sent.

To respond to a Confidential Information Alert

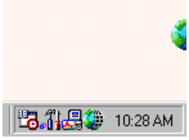
1. In the Confidential Information Alert window, click **Details** to read the information about this event.
2. Do one of the following:
   - Click **Permit this confidential information** to send the information.

     For example, select this option if you are trying to place an order.
   - Click **Block this confidential information** to stop the attempt to send the information.

There is a chance that Norton Internet Security recognizes other information as confidential information. For example, you might be entering a store’s phone number in which the last four digits match the last four digits of your credit card number. In this case, permit the attempt to send the information.

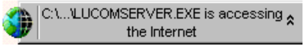
Using Alert Tracker

Alert Tracker keeps you up to date with the actions of Norton Internet Security, and provides a quick way to remove ads from Web pages.



Alert Tracker rests on the side of your screen

When an event occurs that Norton Internet Security wants you to know about, but doesn't need to interrupt your work to tell you, Alert Tracker shows a message for a few seconds and then returns to the side of the screen.



C:\...\LUCOMSERVER.EXE is accessing the Internet

Alert Tracker opens for a few seconds to show messages

Opening Alert Tracker

You can open Alert Tracker to see the most recent messages and to access the Ad Trashcan.

To Open Alert Tracker

- On the Windows desktop, double-click **Alert Tracker**.

For more information, see "Blocking specific ads" on page 78.

Reviewing recent Alert Tracker messages

To review recent Alert Tracker messages

1. On the Windows desktop, double-click **Alert Tracker**.
2. To the right of the first message, click the up arrow if it appears.
3. Click on a message to see the Event Log.

Moving Alert Tracker

Alert Tracker attaches to either side of the screen on your primary monitor.

To move Alert Tracker

- Drag the half globe to the side of the screen where you want it to appear.

Hiding Alert Tracker

You can hide Alert Tracker if you don't want it to appear on your screen.

To hide Alert Tracker

- In the notification area of the Windows taskbar, right-click the Norton Internet Security icon, then click **Hide Alert Tracker**.

Adjusting the reporting detail

The Reporting Level controls the amount of information that appears in Alert Tracker and the number of Security Alerts that appear.

Setting the Reporting Level

The Reporting Level slider lets you select Minimal, Medium, or High Reporting levels. When you change the slider position, the reporting level changes.

Setting	Description
High	Provides the most complete information about Norton Internet Security activities. Shows the most Alert Tracker messages. Notifies you of blocked Web site content, applications accessing the Internet, and Security Alerts.

Setting	Description
Medium (recommended)	Provides information about important Internet events. Shows a medium number of Alert Tracker messages. Notifies you of Security Alerts and Automatic Internet Access Control alerts.
Minimal	Provides information about critical Internet events. Notifies you of Security Alerts and Automatic Internet Access Control alerts.

To set the Reporting Level

1 On the left side of the Norton Internet Security window, click **Internet Status > Reporting**.

2 Move the slider to the Reporting Level that you want.

CHAPTER 8

Customizing firewall protection

Norton Personal Firewall protects your computer from unauthorized access attempts. It blocks attacks from other computers and controls Internet access for applications on your computer.

The firewall provides four types of protection:

- Norton Personal Firewall provides an overall Security Level setting that makes appropriate adjustments throughout the program.
- Internet Access Control sets access rules for the applications on your computer.
- Internet Zone Control lets you access trusted computers and completely block restricted computers.
- Intrusion Protection monitors hacker attacks on your computer and blocks computers that attack you from further access.

Setting the Security Level

The Security Level makes settings throughout Norton Personal Firewall that are appropriate to the Security Level that you select. It changes the firewall setting, and the settings for Java applets and ActiveX controls. It controls whether unused ports respond to access attempts.

The slider lets you select Minimal, Medium, or High security settings. When you change the slider position, the protection level changes.

Setting	Description
High	Firewall is set to High, which blocks everything until you allow it. If you have done an Application Scan, you should not be interrupted frequently with Internet Access Control alerts. ActiveX Control and Java Applet Security is set to Medium, which prompts you each time one is encountered. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Medium (recommended)	Firewall is set to High, which blocks everything until you allow it. If you have done an Application Scan, you should not be interrupted frequently with Internet Access Control alerts. ActiveX Control and Java Applet Security is set to None, which lets all ActiveX controls and Java applets run. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Minimal	Firewall is set to Medium, which blocks connection attempts to Trojan horse programs. ActiveX Control and Java Applet Security is set to None, which lets all ActiveX Controls and Java applets run.

For more information, see "Scanning for Internet-enabled applications" on page 98.

To set the Security Level

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Move the slider to the Security Level that you want.

Making custom security settings

If the Security Level options do not meet your needs, you can change the settings for the Firewall, Java, and ActiveX protection levels.

Changing the Personal Firewall setting

The firewall monitors communications between your computer and other computers on the Internet. It monitors both connection attempts from other computers and attempts by applications on your computer to connect to other computers.

Norton Personal Firewall has three settings:

Setting	Description
High	Blocks all communication that you do not specifically allow. You must create firewall rules for every application that requests Internet access. If you have done an Application Scan, you should not be interrupted frequently with Internet Access Control alerts.
Medium	Blocks many ports used by harmful applications. However, it can also block useful applications when they use the same ports.
None	Disables the firewall and allows all Internet communications.

For more information, see "Scanning for Internet-enabled applications" on page 98.

To change the Personal Firewall setting

1 On the left side of the Norton Internet Security window, click **Personal Firewall** > **Personal Firewall Settings**.

2 Click **Custom Level**.

3 Select the Personal Firewall setting that you want.

Setting Java and ActiveX Security Levels

Java applets and ActiveX controls make Web sites more interactive. Many Web sites rely on ActiveX controls and Java applets to perform and appear correctly. Most of these applications are safe and do not threaten your system or data.

However, ActiveX controls can have total access to your data, depending on how they are programmed. They can copy data from your hard disk and transmit it over the Internet while you are online. They can delete files, intercept messages, capture passwords, or gather banking numbers and other important data.

The only way to prevent bad applications from running on your computer is to block them from downloading. However, blocking all Java applets and ActiveX controls prevents many Web sites from appearing or running correctly.

In the Customize Security Settings dialog box, the Java Applet Security and ActiveX Control Security features have three options:

Setting	Description
High	Blocks your browser from running any Java applets or ActiveX controls over the Internet. This is the safest, but most inconvenient option. Web sites that rely on these elements might not operate properly using this setting.
Medium	Prompts you when Java applets and ActiveX controls are encountered. This lets you temporarily or permanently allow or block each Java applet or ActiveX control that you encounter. It can be bothersome to respond every time you come across a Java applet or ActiveX control, but it lets you decide which ones to run.
None	Lets Java applets and ActiveX controls run whenever you encounter them.

To set Java and ActiveX security levels

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Click **Custom Level**.
3. Select the Java Applet Security setting or ActiveX Control Security setting that you want.

Enabling Internet Access Control alerts

Internet Access Control alerts give you control when an application tries to connect to the Internet but no firewall rule exists for it. When a connection attempt is made, an Internet Access Control alert appears, and you can permit or block the application from accessing the Internet.

Disable this option to block applications from accessing the Internet when there are no specific firewall rules in place for them.

To enable Internet Access Control alerts

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Click **Custom Level**.
3. Check **Enable Access Control Alerts**.

Enabling alerts for unused ports

Norton Internet Security blocks access to the unused ports on your computer.

For example, if someone tries to connect to your computer using Symantec pcAnywhere and you don’t have a pcAnywhere host running, no response is made to acknowledge the connection attempt so the inquiring computer learns nothing.

You can see alerts when an attempt is made to access an unused port on your computer. These alerts are useful for solving problems when you are configuring advanced programs and features such as Internet Connection Sharing. Disable to avoid alerts about harmless connection attempts.

To enable alerts for unused ports

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Click **Custom Level**.
3. Check **Alert when unused ports are accessed**.

Controlling applications that access the Internet

Applications access the Internet for many reasons. Your Web browser accesses the Internet so that you can view Web pages. LiveUpdate accesses the Internet to retrieve program and protection updates for your Symantec products. Microsoft NetMeeting accesses the Internet to let you conduct meetings over the Internet.

Each of these applications has different requirements for accessing the Internet. Some, such as LiveUpdate, have simple requirements. Others, such as Internet Explorer, have complex requirements.

Internet Access Control maintains a list of the applications on your computer that access the Internet. The list records the applications' requirements, and whether Internet access is allowed or blocked.

There are several ways to add applications to the Internet Access Control list:

- Scan for Internet-enabled applications: Finds and configures access for all of your Internet-enabled applications at once.

  For more information, see "Scanning for Internet-enabled applications" on page 98.

- Enable Automatic Internet Access Control: Automatically configures access for well-known applications the first time that you run them.

  For more information, see "Enabling Automatic Internet Access Control" on page 99.

- Respond to alerts: Norton Internet Security alerts you the first time each Internet-enabled application attempts to access the Internet. You can then allow or block access. If the application is recognized by Norton Internet Security, it suggests that you use the automatic configuration option.

  For more information, see "Responding to Internet Access Control alerts" on page 84.

- Add applications individually: You can add applications to the list on the Internet Access Control screen.

  For more information, see "Adding an application to Internet Access Control" on page 100.

Scanning for Internet-enabled applications

Scanning for Internet-enabled applications is the quickest way to set up Internet Access Control for all of your applications. Norton Internet Security scans your computer for applications that it recognizes and then lets you choose appropriate settings for each application.

To scan for Internet-enabled applications

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Configure**, then click **Application Scan**.
3. Follow the on-screen instructions.

Enabling Automatic Internet Access Control

When Automatic Internet Access Control is enabled, Norton Internet Security automatically creates a new firewall rule for applications that it has digital signatures (fingerprints) for the first time the applications are run.

Disable this option if you want to be notified when a new application attempts to access the Internet.

Be sure to run LiveUpdate weekly to retrieve program and protection updates.

To enable Automatic Internet Access Control

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Configure**, then check **Enable Automatic Internet Access Control**.

Responding to Internet Access Control alerts

If Automatic Internet Access Control is not enabled, or Norton Internet Security encounters an application that it does not recognize attempting to access the Internet, an Internet Access Control alert appears.

If the option Automatically configure Internet access appears in the alert, then Norton Internet Security knows about the application and can configure appropriate access.

If Automatically configure Internet access does not appear, the application is not recognized by Norton Internet Security and you must decide whether or not to allow access to the application. Review the threat level before you make your decision.

If Automatically configure Internet access appears in the alert but is disabled, then Norton Internet Security knows about the application but does not expect the communication attempt as part of the application’s normal operation.

For more information, see “Responding to Internet Access Control alerts” on page 84.

Adding an application to Internet Access Control

You can manually add applications to the list of applications in Internet Access Control. Use this method if you have an application with specific Internet access requirements and you understand firewall rules.

To add an application to Internet Access Control

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Add**.
3. Select the application's executable file.
4. Click **Open**.
5. In the Internet Access Control window, follow the on-screen instructions.

Changing Internet Access Control settings

You can change the Internet Access Control settings for applications. For example, you may decide that you want to allow access to an application that is blocked.

To change Internet Access Control settings

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Access Control**.
2. Under Internet Access, select the entry for the application that you want to change.
3. On the drop-down menu, select a new setting.

Changing system-wide settings

System-wide settings provide protection that is broader than those covering a single application. For example, protection against someone attaching to your computer using Microsoft networking is provided in system-wide settings.

System-wide settings provide a series of rules that the firewall uses to allow or block various activities. While you can add to or change these rules, you should have a good understanding of what they do to ensure that you don't compromise your protection.

To change system-wide settings

1 On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Access Control**.

2 Click **Configure**, then click **System-Wide Settings**.

Home network control with Internet Zone Control

Internet Zone Control provides an easy way for you to identify computers that you trust not to attack you, and computers that you specifically want to restrict from accessing your computer. There are two zones: Trusted and Restricted.

Computers that you place in the Trusted zone are not regulated by Norton Internet Security. They have as much access to your computer as they would have if Norton Internet Security was not installed. Use the Trusted zone for computers on your local network with which you need to share files and printers.

If a computer in your Trusted zone is attacked, and a hacker takes control of it, it poses a risk to your computer.

Computers that you place in the Restricted zone are prevented from accessing your computer at all. Add computers that repeatedly attempt to attack you to the Restricted zone. The Restricted zone provides the highest level of protection, beyond the normal protection provided by Norton Internet Security. You cannot interact with computers in the Restricted zone at all.

Adding computers to zones

Add computers that you trust to the Trusted zone. Add computers that you want to totally block to the Restricted zone.

To add computers to a zone

1 On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Zone Control**.

2 Select the zone to which you want to add a computer.

3 Click **Add**.

You can add a single computer or a group of computers. For more information, see "Identifying computers to Norton Internet Security" on page 106.

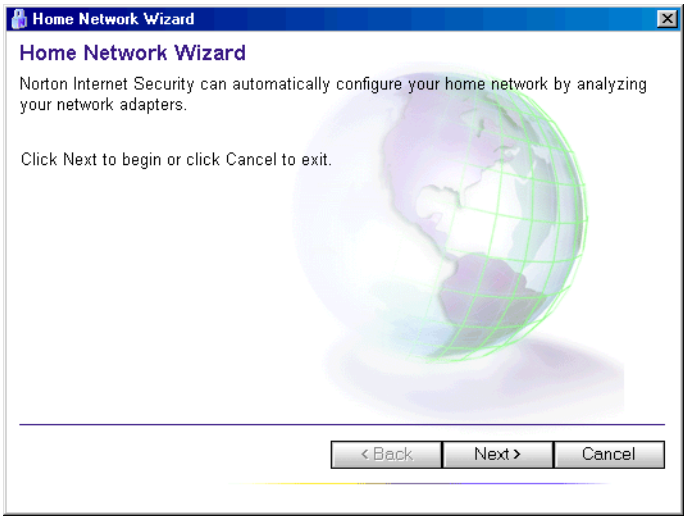
Adding computers on your home network to the Trusted zone

The Home Network Wizard provides the easiest way for you to identify other computers on your home network with which you want to share files or printers.

To add the computers on your home network to the Trusted zone

1 On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Zone Control**.

2 In the Internet Zone Control pane, click **Wizard**.

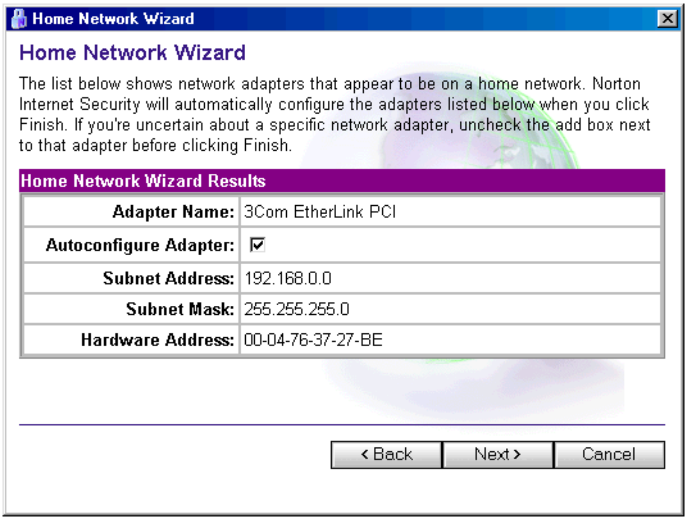


Home Network Wizard

Norton Internet Security can automatically configure your home network by analyzing your network adapters.

Click Next to begin or click Cancel to exit.

3 Click **Next** to begin the Wizard.



Home Network Wizard

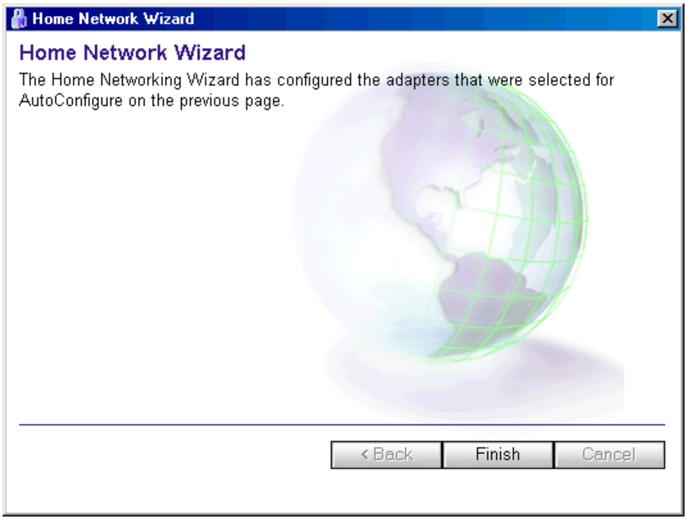
The list below shows network adapters that appear to be on a home network. Norton Internet Security will automatically configure the adapters listed below when you click Finish. If you're uncertain about a specific network adapter, uncheck the add box next to that adapter before clicking Finish.

Home Network Wizard Results

Adapter Name:	3Com EtherLink PCI
Autoconfigure Adapter:	☑
Subnet Address:	192.168.0.0
Subnet Mask:	255.255.255.0
Hardware Address:	00-04-76-37-27-BE

4 In the resulting list, check the network adapters that you want configured automatically and added to your Trusted zone.

5 Click **Next**.



Home Network Wizard

The Home Networking Wizard has configured the adapters that were selected for AutoConfigure on the previous page.

6 Click **Finish** to close the Home Network Wizard.

Using Intrusion Protection to stop attacks

Intrusion Protection stops hacker attacks as they occur. Norton Internet Security monitors Internet communications, looking for patterns of communications that are typical of a hacker attack. For example, if a computer tries to connect to a series of ports on your computer, Intrusion Protection recognizes it as a port scan, which is a common method of finding weaknesses to attack.

Intrusion Protection also detects attempts to connect to ports used by remote-access Trojan horse programs.

For more information, see "Understanding Internet risks" on page 151.

You can review and control the reaction to attacks in the Intrusion Protection window.

Detecting Port Scan Attempts

To be notified when Norton Internet Security detects a port scan or other attack, enable Detect Port Scan Attempts.

To enable Detect Port Scan Attempts

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Intrusion Protection**.
2. Check **Detect Port Scan Attempts**.

Enabling AutoBlock

When Norton Internet Security detects an attack, it warns you and blocks all communications from the attacking computer for 30 minutes. This automatic blocking of communications is called AutoBlock.

AutoBlock stops all communication from the remote computer for 30 minutes. It does not stop you from communicating to the remote computer.

Computers in the Trusted and Restricted zones are not subject to AutoBlock. Computers in the Trusted zone are never blocked, while computers in the Restricted zone are permanently blocked.

To enable AutoBlock

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Intrusion Protection**.
2. Check **Enable AutoBlock**.

Unblocking a blocked computer

In some cases, Norton Internet Security may recognize normal activity as an attack. If you can't communicate with a computer with which you should be able to communicate, see if it is on the list of Computers currently blocked by AutoBlock.

If a computer that you need to access appears on the list of Computers currently blocked by AutoBlock, unblock it.

To unblock a single blocked computer

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Intrusion Protection**.
2. Select the IP address of the computer that you want to unblock.
3. Click **Unblock**.

Excluding specific activities from AutoBlock

Some normal Internet activities will be repeatedly recognized by Norton Internet Security as an attack. For example, some Internet service providers scan the ports of client computers to ensure that they are within their service agreements.

To prevent normal activities from interrupting your Internet use, you can exclude these activities from being blocked by AutoBlock.

To exclude activities from AutoBlock

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Intrusion Protection**.
2. Click **Exclusions**.
3. In the Currently blocked list, select the IP address that you want to exclude.
4. Click **Exclude**.

Restricting a blocked computer

You can add a blocked computer to your Restricted zone to permanently prevent that computer from accessing your computer. Computers added to the Restricted zone do not appear on the blocked list.

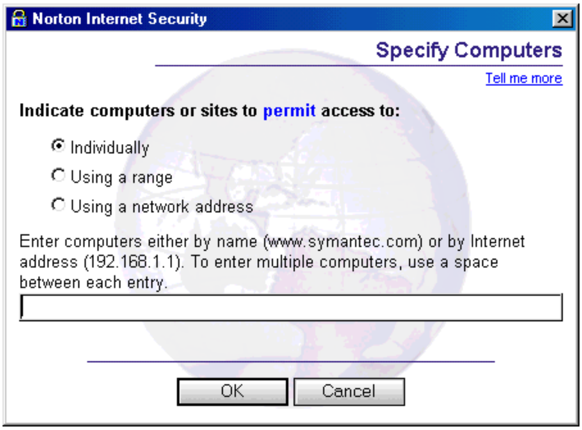
To restrict a blocked computer

1 On the left side of the Norton Internet Security window, click **Personal Firewall** > **Intrusion Protection**.

2 In the list of computers currently blocked by AutoBlock, select the computer to add to the Restricted zone, then click **Restrict**.

Identifying computers to Norton Internet Security

There are several places in Norton Internet Security in which you might need to identify computers to the program. In each case, the Specify Computers dialog box appears.



Indicate computers or sites to permit access to:

● Individually
○ Using a range
○ Using a network address

Enter computers either by name (www.symantec.com) or by Internet address (192.168.1.1). To enter multiple computers, use a space between each entry.

The Specify Computers dialog box lets you specify computers in three ways. In each you can use IP addresses to identify computers.

For more information, see "About the Internet" on page 143.

Specifying individual computers

IP addresses are 32-bit numbers expressed as four decimal numbers, each ranging from 0 to 255, and separated by periods. For example: 206.204.52.71.

The computer name that you type can be a URL (Uniform Resource Locator), such as service.symantec.com, or a Microsoft Network computer name, such as Mojave. You can find the names of computers on your local network in Network Neighborhood or Network Places.

Note: If you don't have TCP/IP bound to Client for Microsoft Networks in Windows Network Properties, you must use IP addresses instead of names for the computers on your local network.

To specify an individual computer

1. In the Specify Computers window, click **Individually**.
2. Type the name or IP address of a single computer.

Specifying a range of computers

You can enter a range of computers by specifying the starting (lowest numerically) IP address and the ending (highest numerically) IP address. All of the computers within that range of IP addresses are included.

In almost every case, the first three of the four numbers of the IP addresses entered should be the same.

To specify a range of computers

1. In the Specify Computers window, click **Using a range**.
2. In the Starting Internet Address field, type the starting (lowest numerically) IP address.
3. In the Ending Internet Address field, type the ending (highest numerically) IP address.

Specifying computers using a network address

You can identify all the computers on a single subnet by specifying an IP address and a subnet mask.

The IP address you specify can be any address in the subnet that you are identifying. The appropriate subnet mask is almost always 255.255.255.0.

For more information, see "How computers are identified on the Internet" on page 149.

To specify computers using a network address

1 In the Specify Computers window, click **Using a network address**.

2 In the Network Address field, type the IP address of a computer on the subnet.

3 In the Subnet Mask field, type the subnet mask.

CHAPTER 9

Handling virus emergencies

The complete Norton AntiVirus User’s Guide and this user’s guide are included on the Norton Internet Security CD in the Manual folder. These guides are in Adobe Acrobat Portable Document Format (.pdf), and require the Adobe Acrobat Reader to view them. An Adobe Acrobat Reader application is located in the Manual folder on the Norton Internet Security CD. While this section will help you resolve most virus emergencies, for complete instructions on using Norton AntiVirus, see the Norton AntiVirus User’s Guide in the Manual folder.

What to do if a virus is found

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

If a Norton AntiVirus alert appears on your screen, and you are not sure what option to select, use this table to decide what to do.

For more information, see “Types of virus alerts” on page 110.

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 to use them
Repair	Eliminates the virus and repairs the infected item. When a virus is found, Repair is always the best choice.
Quarantine	Isolates the virus-infected file, but does not remove the virus. Click 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.
Delete	Erases both the virus and the infected file. The virus and file are gone forever. Click Delete if Norton AntiVirus cannot repair the file. Replace a deleted file from the original application disks or backup copy. If the virus is detected again, your backup copy or original disk is infected.
Stop	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 attempt to use the infected file.
Continue	Continues the current operation. Click 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, click Stop.
Exclude	If you click 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

There are several types of virus alerts:

- Virus Found
- Virus in Memory
- Virus-Like Activity

Virus Found

When Norton AntiVirus finds that one of your files has been infected by a virus, a warning message appears.

For example:

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

To get rid of a virus infection

- Press **R** for Repair.

The file is restored to exactly the way it was before the virus infected it. 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 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 other files.

When Norton AntiVirus finds a virus in memory, a warning message appears.

For example:

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.

If you do not have Rescue Disks, you can use Emergency Disks.

For more information, see “Using Emergency Disks in virus emergencies” on page 115.

To eliminate a virus in memory

1. Shut down your computer, using the power switch.
2. Insert your Rescue Boot Disk into drive A.
3. After waiting a few seconds, restart the computer.
4. Follow the on-screen instructions.

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 the following:

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 a file

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 with LiveUpdate and scan again.
- Read the information on your screen carefully to identify the type of item that cannot be repaired, and then match it to one of the types below:
  - Infected files are those with filename extensions such as .exe, .doc, .dot, or .xls. Files with any name can be infected.
  - Hard disk master boot record, boot record, or system files (such as Io.sys or Msdos.sys) and floppy disk boot record and system files are replaced using the 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.

Some infections can be removed by special removal tools that are on the Norton Internet Security CD in the Support\NAVTools\Repair folder. These tools are also available on the Symantec Web site at http://www.symantec.com/avcenter/.

If Norton AntiVirus cannot repair a file

- Do one of the following:
  - Click **Quarantine** (recommended).

    After the file is quarantined, you can update your virus definitions and scan again or submit the file to SARC for analysis.
  - Click **Delete**.

    Replace the deleted document file with a backup copy or reinstall a deleted application from the original application 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 application disks are infected. Contact the publisher for a replacement disk.

Hard disk master boot record or boot record

Hard disk master boot record, boot record, and system files (such as Io.sys or Msdos.sys) are replaced using the Rescue Disks or, sometimes, your operating system (Windows or DOS) disks.

If Norton AntiVirus cannot repair your hard disk or master boot record, use your up-to-date Rescue Disks to restore it.

If your Rescue Disks are not up-to-date, contact Symantec Technical Support.

For more information, see “Service and support solutions” on page 161.

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 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 be removed only if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus alert tells 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 disk partitions (with software such as Partition-It or Partition Magic)
- Upgraded your operating system (to Windows Me, for example)

Warning: If the critical information stored on the Rescue Disks is outdated, it can cause problems when you attempt to restore your computer. It is unlikely you will be able to fix these problems on your own. However, if you have current Rescue Disks, the following procedure is safe to attempt.

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

If your Rescue Disks are not current, 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. Insert the Basic Rescue Boot floppy disk into the floppy disk drive and restart your computer.

   The Rescue program runs in DOS.

2. Use the arrow keys to highlight the program that you want to run.

   A description of the highlighted program appears in the right panel of the Rescue program. Your choices are:

   - Norton AntiVirus. Scans your computer for viruses and repairs any infected files.
   - Rescue Recovery. Checks and restores boot and partition information.

3. Press **Enter** to run the highlighted program.
4. Follow the on-screen instructions for inserting and removing the Rescue Disks.
5. When the Rescue program is done, remove the Rescue Disk in the floppy disk drive and restart your computer.

Using Emergency Disks in virus emergencies

Emergency Disks can be used to solve virus emergencies if you have not made Rescue Disks. Rescue Disks are always a better solution because they include information that is specific to the computer on which they were made. For more information, see "Creating Emergency Disks" on page 22.

You can use the CD that contains Norton Internet Security as an Emergency Disk if your computer can start from the CD-ROM drive. For more information, see "Using the CD as an Emergency Disk" on page 116.

Using Emergency Disks

Use Emergency Disks to solve virus emergencies if you have not made Rescue Disks.

To use the Emergency Disks

1 Insert Emergency Disk 1 into the floppy disk drive and restart your computer.

The Emergency program runs in DOS.

2 Ensure that Antivirus is selected and press **Enter** to begin the Norton AntiVirus Emergency program.

3 Follow the on-screen instructions for inserting and removing the Emergency Disks.

The Emergency program automatically scans your computer and removes viruses.

4 When the Emergency program is done, remove the Emergency Disk in the floppy disk drive and restart your computer.

Using the CD as an Emergency Disk

If you are using the Norton Internet Security CD as an Emergency Disk, use this procedure whenever you are instructed to insert Emergency Disk 1. You can ignore all instructions to change disks, as all necessary information is on the CD.

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

To use the Norton Internet Security CD as an Emergency Disk

1 Insert the Norton Internet Security CD into the CD-ROM drive.

2 Restart your computer.

The Emergency program scans your computer and removes viruses.

Submitting files to Symantec

If you suspect that your computer has a virus, but Norton AntiVirus does not detect a virus after you have used LiveUpdate to get the latest virus definitions, your computer might have a new type of virus.

Place the suspect file in Quarantine. This ensures that the virus doesn't spread. Then, use Scan and Deliver to submit the file to Symantec.

Submitting a sample of a suspected virus to Symantec for testing is a two-step process:

- Place the file in Quarantine.
- Submit the quarantined file to Symantec.

Placing a file in Quarantine

The first step in submitting a file to Symantec is to place the file in Quarantine.

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

To place a file in Quarantine

1. Start Norton Internet Security.
2. In the Norton Internet Security main window, click **Norton AntiVirus** > **Reports**.
3. On the Quarantined items line, click **View Report**.
4. In Norton AntiVirus Quarantine, click **Add Item**.
5. In the Add to Quarantine dialog box, browse to and select the file that you want to place in Quarantine.
6. Click **Add**.

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

Submitting a quarantined file to Symantec

Once you have a file in Quarantine, you can submit it to Symantec for testing.

To submit a quarantined file to Symantec

1 In the right pane of the Quarantine window, select the file that you want to submit.

2 Click **Submit Item**.

3 Follow the on-screen instructions.

CHAPTER 10

Monitoring Norton Internet Security events

Norton Internet Security provides information about its activities.

- The Current Status window shows several sets of counters indicating current Web- and firewall-related activities.
- The Event Log records actions that Norton Internet Security has taken and records your Internet activities.
- The Statistics window displays statistics of network activity and actions that Norton Internet Security has taken.

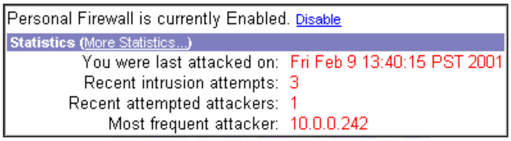
Reviewing Current Status

Current Status gives you a view of the current state of Norton Internet Security. It displays status for the following:

- Personal Firewall
- Privacy
- Ad Blocking
- Parental Control

Checking Personal Firewall status

Personal Firewall status provides information about recent attacks on your computer, including the time of the most recent attack and the IP address of the computer that attacked you.



Personal Firewall is currently Enabled. Disable

Statistics (More Statistics...)	
You were last attacked on:	Fri Feb 9 13:40:15 PST 2001
Recent intrusion attempts:	3
Recent attempted attackers:	1
Most frequent attacker:	10.0.0.242

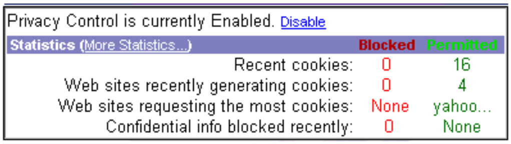
To check Personal Firewall status

1 On the left side of the Norton Internet Security window, click **Internet Status** > **Current Status**.

2 Click **Personal Firewall**.

Checking Privacy status

Privacy Control status shows you how many cookies have been blocked or permitted, and how many times you have sent or blocked confidential information.



Privacy Control is currently Enabled. Disable

Statistics (More Statistics...)	Blocked	Permitted
Recent cookies:	0	16
Web sites recently generating cookies:	0	4
Web sites requesting the most cookies:	None	yahoo...
Confidential info blocked recently:	0	None

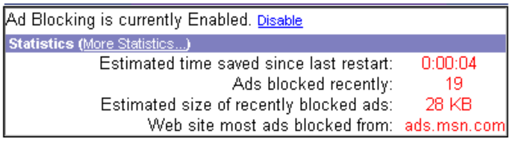
To check privacy status

1 On the left side of the Norton Internet Security window, click **Internet Status** > **Current Status**.

2 Click **Privacy Control**.

Checking Ad Blocking status

Ad Blocking status shows how many ads have been blocked and the amount of time you have saved while browsing the Internet.



Ad Blocking is currently Enabled. Disable

Statistics (More Statistics...)

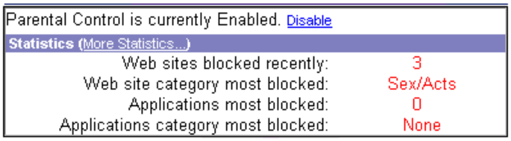
Estimated time saved since last restart:	0:00:04
Ads blocked recently:	19
Estimated size of recently blocked ads:	28 KB
Web site most ads blocked from:	ads.msn.com

To check Ad Blocking status

1. On the left side of the Norton Internet Security window, click **Internet Status** > **Current Status**.
2. In the middle of the window, click **Ad Blocking**.

Checking Parental Control status

Parental Control status shows how many Web sites and applications have been blocked.



Parental Control is currently Enabled. Disable

Statistics (More Statistics...)

Web sites blocked recently:	3
Web site category most blocked:	Sex/Acts
Applications most blocked:	0
Applications category most blocked:	None

To check Parental Control status

1. On the left side of the Norton Internet Security window, click **Internet Status** > **Current Status**.
2. In the middle of the window, click **Parental Control**.

CHAPTER 11

Configuring Norton Internet Security for common situations

Norton Internet Security can be configured to meet your needs in many different situations. This section describes the appropriate settings for a number of common situations.

Using Norton Internet Security with a dial-up connection

As installed, Norton Internet Security is properly configured to provide protection with a dial-up connection.

Enable Ad Blocking to speed up your Internet browsing.

Using Norton Internet Security with a broadband connection

As installed, Norton Internet Security is properly configured to provide protection with a broadband connection, such as a cable modem or DSL service.

The most important thing in maintaining your protection from Internet risks is to keep Norton Internet Security enabled. Because most broadband connections are always active, your computer can be attacked at any time.

Troubleshooting broadband problems

Common broadband problems include:

- NetBIOS name is required.
- ISP periodically scans your computer.

NetBIOS name is required

A few cable systems require that your computer make its NetBIOS name visible. The NetBIOS name is visible, while the files and folders on your computer remain hidden.

To make your NetBIOS name visible

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Configure** and select **System-Wide Settings**.
3. In the System-Wide Settings dialog box, select Default Inbound NetBIOS Name, then click **Modify**.
4. On the Action tab of the Modify Rule dialog box, click **Permit Internet access**.
5. Click **OK**.
6. In the System-Wide Settings dialog box, click **OK**.

ISP periodically scans your computer

Some broadband systems scan the ports on users' computers to ensure that they are keeping to their service agreements. Norton Internet Security might interpret this as a malicious port scan and stop communications with your ISP.

If this occurs, follow these steps to allow ISP port scans.

To allow ISP port scans

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Intrusion Protection**.
2. In the Intrusion Protection window, click **Exclusions**.
3. In the Exclusions dialog box, select the ISP that is currently blocked, then click **Exclude**.
4. Click **OK**.

Using Norton Internet Security in a family

Norton Internet Security Parental Control helps you protect your children from the risks of the Internet.

With one child or children close in age

If you have one child, or your children's needs are similar, you can create a single account. Adults in the family can use the supervisor account, and the child or children can use the children's account.

For more information, see "Understanding accounts" on page 53.

With multiple children or wider age differences

If your children's needs vary, create an account for each child. This lets you tailor the settings to the specific needs of each child.

For more information, see "About family accounts" on page 57.

Using Norton Internet Security with multiplayer games

Some multiplayer games require special Internet access. If you have trouble with your games, give the game application full permission to access the Internet. If that doesn't work, temporarily put the computers of the other players in the Trusted zone.

Giving a multiplayer game access to the Internet

The first step to making a multiplayer game work is to give it permission to access the Internet.

To give a multiplayer game access to the Internet

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Add**.
3. Select the application's executable file, then click **Open**.
4. In the Internet Access Control window, click **Permit <application> access to the Internet**.
5. Click **OK**.

Note: If the application is already listed, click its entry under Internet Access and choose Permit All.

Placing other players in the Trusted zone

If giving the game application access to the Internet doesn't work, temporarily place the computers of the other players in your Trusted zone.

To place other players in the Trusted zone

1. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Zone Control**.
2. On the Trusted tab, click **Add**.
3. Enter the IP addresses of the other players.

Using Norton Internet Security on a home network

Norton Internet Security protects you from Internet risks while allowing you full use of your local network.

For your safety, Norton Internet Security prevents local network activity when it is installed. This prevents someone from connecting to your computer over the Internet using Microsoft Networking.

Enabling file and printer sharing

Microsoft networking provides file and printer sharing. You can enable these features on your local network, while protecting them from the Internet.

To enable file and printer sharing

1 Open Windows Explorer.

2 Expand **Network Neighborhood** or **My Network Places** to locate the names of the computers on your local network.

3 On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Zone Control**.

4 On the Trusted tab, click **Add**.

5 Add each of the local computers to the Trusted zone.

For more information, see “Adding computers to zones” on page 101.

You can also unblock file and printer sharing using the System-Wide Settings.

To unblock file and printer sharing

1 On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Access Control**.

2 Click **Configure** and select **System-Wide Settings**.

3 In the System-Wide Settings dialog box, select the entry for Windows file sharing or printer sharing, then click **Modify**.

4 On the Action tab of the Modify Rule dialog box, click **Permit Internet access**.

5 Click **OK**.

6 In the System-Wide Settings dialog box, click **OK**.

Internet connection sharing

Norton Internet Security works with Internet connection sharing.

For full protection, install Norton Internet Security on each computer on your home network. Installing Norton Internet Security on the gateway computer protects your network from many outside attacks, but cannot protect against Trojan horses or other problem applications that initiate outbound connections unless it is installed on each computer on the network.

Using Norton Internet Security with a cable or DSL router

Norton Internet Security works behind a cable or DSL router and adds to the protection provided by the router. In some cases, you might want to reduce the protection provided by the router so that you can use applications like NetMeeting or Microsoft Messenger.

Norton Internet Security also provides features that might not be available with cable and DSL routers, such as privacy protection.

Using Norton Internet Security on a corporate network

If you use your computer at home and at work, you might need to use Norton Internet Security behind a corporate firewall.

Enabling file and printer sharing

If you don’t want to disable Norton Internet Security, you can enable file and printer sharing so your computer works on an office network.

To enable file and printer sharing

1. Open Windows Explorer.
2. Expand **Network Neighborhood** or **My Network Places** to locate the names of the computers on your local network.
3. On the left side of the Norton Internet Security window, click **Personal Firewall** > **Internet Zone Control**.
4. On the Trusted tab, click **Add**.
5. Add each of the local computers to the Trusted zone.

For more information, see “Adding computers to zones” on page 101.

You can also unblock file and printer sharing. For more information, see “To unblock file and printer sharing” on page 127.

Administrative software on corporate networks

Administrative software used on some corporate networks may cause alerts from Norton Internet Security. If you experience unusual alerts while working on a corporate network, disable Norton Internet Security or talk to your network administrator.

Using Norton Internet Security with a proxy server

Norton Internet Security works with most proxy servers. However, you might have to change some settings to maintain full protection.

Determining whether Norton Internet Security works with your proxy server

The first step in making this determination is to find out if Norton Internet Security works with your proxy server.

To determine whether Norton Internet Security works with your proxy server

1. At the top of the Norton Internet Security window, click **Options**.
2. Click **Internet Security**.
3. Click **View Statistics**.
4. In the Web category, look at the Bytes Processed counter.
5. Use your browser to connect to a Web site.

   If Norton Internet Security is filtering, the Bytes Processed counter in the Statistics window should increase as you access Web pages. If the Bytes Processed counter stays at 0, then Norton Internet Security is probably not monitoring the port used by your proxy server.

Determining which port to monitor for HTTP communication

If Norton Internet Security does not work with your proxy server, check the port that your proxy server is using for HTTP communications.

To determine which port to monitor for HTTP communication

1. Use your browser to connect to a Web site.
2. At the top of the Norton Internet Security window, click **Options**.
3. Click **Internet Security**.
4. Click **View Event Log**.
5. On the Connections tab, look at the information in the Remote column.

   There should be a port number following the IP address of the site that you viewed with your browser. This number is the port number that was used to access your proxy server for your Web connection.
6. Record the port number.

Specifying which ports to monitor for HTTP communication

Your computer may connect to the Internet through a proxy server, which causes all HTTP communication to go through the port used by the proxy server.

To specify which ports to monitor for HTTP communication

1 At the top of the Norton Internet Security window, click **Options**.

2 Click **Internet Security**.

3 Click **Advanced Options**.

4 On the Other tab, do one of the following:

- Click **Add**, then enter the number of the port that you want to monitor for HTTP communication to add a port to the HTTP Port List.
- Select the port number in the HTTP Port List, then click **Remove** to remove a port from the HTTP Port List.

Running a Web server with Norton Internet Security

When properly configured, Norton Internet Security will not prevent you from running a Web server.

To allow a Web server to run behind Norton Internet Security, you must create a rule that allows inbound TCP connections on port 80.

To configure Norton Internet Security for a Web server

1 View your Web site by entering the IP address in the address bar of your browser.

Norton Internet Security displays an Internet Access Control alert.

2 In the alert dialog box, click **Automatically configure Internet access**.

Running an FTP server with Norton Internet Security

To allow an FTP server to run behind Norton Internet Security, you must create the following:

- A rule that allows inbound TCP connections on port 21
- A rule that allows outbound TCP connections on port 22
- A rule that allows inbound TCP connections on ports 1024 to 5000

To configure Norton Internet Security for an FTP server

1. View your FTP site by typing **FTP://** followed by the IP address of your FTP server in the address bar of your browser.

   Norton Internet Security displays an Internet Access Control alert.

2. In the alert dialog box, click **Customize Internet access for this application**.

   For more information, see “Responding to Internet Access Control alerts” on page 84.

Using Norton Internet Security with DHCP

If your computer gets its IP address from a DHCP server that provides a different IP address each time, you need to be careful when you enter local addresses in rules.

Instead of entering a single IP address, which might change at any time, enter a network address using a base IP address and a subnet mask. Enter values that cover the range of addresses that might be assigned to your computer.

For more information, see “Identifying computers to Norton Internet Security” on page 106.

Using Norton Internet Security with pcAnywhere

You should have no problems using pcAnywhere as either a client or host with Norton Internet Security. The first time you run it, or during an application scan, Norton Internet Security identifies pcAnywhere and creates Internet access rules automatically.

For maximum protection, if you run pcAnywhere host, edit the rule to limit its use to only the computers with which you use it. This, coupled with pcAnywhere passwords, provides maximum security.

Using Norton Internet Security with a VPN

Norton Internet Security works with the following Virtual Private Networks (VPNs):

- Nortel
- VPNRemote
- PGP
- SecureRemote

With most VPNs, when the VPN client is active, you cannot see the Internet or other computers on your local network. You can only see what is available through the VPN server to which you are connected.

CHAPTER 12

Troubleshooting

This section can help you solve many common problems. If you don't find your solution here, you might find a solution elsewhere in this document.

For more information, see "Configuring Norton Internet Security for common situations" on page 123.

Troubleshooting Norton Internet Security problems

Following are solutions to problems that might occur with Norton Internet Security.

What is wrong with this Web site?

Running Norton Internet Security can block certain elements of a Web site that prevent it from displaying correctly in your Web browser. In some cases, the site might not display at all.

In most cases, this is Norton Internet Security protecting you from inappropriate content. Your best solution may be to go to another, more appropriate Web site.

To see if Norton Internet Security is blocking access to the Web site, disable Norton Internet Security and try the Web site again. Keep in mind that, when you disable Norton Internet Security, you are turning off the protection it provides to prevent private information from being sent, and inappropriate information from being received.

For more information, see “Temporarily disabling Norton Internet Security” on page 36.

If you cannot connect with Norton Internet Security disabled, there might be a problem with the Internet or your Internet Service Provider.

It could be blocking cookies

Many Web sites require that cookies be enabled on your computer to display correctly. If you have cookie blocking turned on and the Web page appears to be blank, turn off cookie blocking and try the page again.

To stop blocking cookies

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click **Custom Level**.
3. Set **Cookie Blocking** to Medium or None.

If this fixes the problem, consider making site-specific settings to allow cookies from that site.

It could be parental controls

If you have set up Parental Control to block certain categories of Web sites, it may be blocking the site you are attempting to view. When Parental Control blocks a site, it always displays a message telling you that the site is blocked.

Consider creating an exception to the list of sites blocked by Parental Controls.

For more information, see “Restricting access to Web sites” on page 64.

It could be a firewall rule

A firewall rule might be blocking the Web site. When this happens, you will usually see a message saying that you could not connect. You can view the firewall rules that have been set up and determine if a rule is blocking the site.

It could be ad blocking

Sometimes blocking advertisements on the Internet prevents an entire Web site from appearing in your browser. If you suspect this is happening, turn off Ad Blocking and try the site again.

For more information, see "Blocking Internet advertisements" on page 77.

If this fixes the problem, consider making site-specific settings to allow ads from that site.

It could be ActiveX or Java blocking

Some Web sites display only ActiveX controls or Java applets. If you are blocking them, nothing appears on these sites.

For more information, see "Setting Java and ActiveX Security Levels" on page 95.

If this fixes the problem, consider making site-specific settings to allow ActiveX controls or Java applets from that site.

It could be script blocking

Some Web sites use JavaScript in their navigation controls and in other places. If Norton Personal Firewall is blocking JavaScript or VB Script, it may cause problems with these Web sites.

To stop blocking JavaScript or VB Scripts

1. At the top of the Norton Internet Security window, click **Options**.
2. Click **Internet Security**.
3. Click **Advanced Options**.
4. On the Web tab, click the **Active Content** tab.
5. In the list of Web sites do, one of the following:
   - Select the Web site that you want to change.
   - Click **(Defaults)** to change all unlisted Web sites.
6. In the Script box, select **Allow All Scripts To Execute**.

Why can’t I post information online?

If you are unable to post information to a Web site, it may be because Privacy Control is blocking the information. Check the Confidential Information list on the Privacy window to see if the information you are trying to enter is being blocked.

To check the information on the Personal Information list

1. On the left side of the Norton Internet Security window, click **Privacy Control**.
2. Click **Confidential Info**.

   This opens the list of information that Privacy Control blocks from being transferred to the Internet.

Why won’t an application connect to the Internet?

A restricted account user might not be able to use an application with the Internet for any of the following reasons:

- The application might belong to a category of applications that is restricted for this account.

  For more information, see “Blocking applications from accessing the Internet” on page 66.

- You may be using a restricted account and there is no firewall rule allowing the application to create a connection to the Internet. If a firewall rule does not exist for the connection, the attempt is automatically denied without notification for restricted accounts.

  For supervisor and normal accounts, having no firewall rule triggers an Internet Access Control alert, allowing the program to create a new firewall rule for the new connection. For more information, see “Responding to Internet Access Control alerts” on page 84.

  Users with normal or supervisor rights can change the current account to a supervisor or normal account. Then, they can run the application to make an Internet Access Control alert appear. After setting up a firewall rule, they should set the active user account back to the restricted user’s account name. The restricted user can then run the application that accesses the Internet.

- Norton Internet Security could be blocking your account from using this application on the Internet. If it is, the supervisor can change your account settings to stop blocking it.

  For more information, see “Setting up account restrictions” on page 63.

Why doesn’t Norton Internet Security notify me before letting applications access the Internet?

If Automatic Internet Access Control is enabled, Norton Internet Security creates rules for applications it recognizes without notifying you. You can disable Automatic Internet Access Control.

For more information, see “Enabling Automatic Internet Access Control” on page 99.

For more information, see “Adjusting the reporting detail” on page 90.

Why doesn’t my local network work?

Norton Internet Security blocks the use of Microsoft networking to prevent someone from attaching to your computer across the Internet.

To allow the use of your local network, including file and printer sharing, place the computers on your local network in the Trusted zone or unblock access using System-Wide Settings.

For more information, see “Adding computers on your home network to the Trusted zone” on page 102.

For more information, see “Using Norton Internet Security on a home network” on page 126.

Why can’t I print to a shared printer?

Norton Internet Security blocks the use of Microsoft networking to prevent someone from attaching to your computer across the Internet.

To allow the use of your local network, including printer sharing, place the computers on your local network in the Trusted zone.

For more information, see “Adding computers on your home network to the Trusted zone” on page 102.

Why can't LiveUpdate get a list of updates?

The first time that you run LiveUpdate after installing Norton Internet Security, an Internet Access Control alert appears to help you create a rule that allows LiveUpdate to access the Internet. If you are logged in to a restricted account, Norton Internet Security is prevented from creating these rules.

Log on to an account with supervisor privileges and run LiveUpdate. This creates rules that allow anyone to run LiveUpdate in the future.

How can a Web site get my browser information?

The Browser Privacy settings prevent your browser from sending out browser information. However, some diagnostic sites on the Internet might report browser information even though the Browser Privacy settings are blocking the information:

- If you are not blocking Java, ActiveX, or scripts, the site might be using one of these methods to retrieve the information.

  For more information, see "Setting Java and ActiveX Security Levels" on page 95.

- Sometimes when Web servers do not get the information from the browser, they simply use the last piece of browser information they received instead. You might see the information from the last person who viewed the site.

Troubleshooting Norton AntiVirus problems

Following are solutions for problems that might occur with Norton AntiVirus.

My Rescue Disk does not work

Because of the number of product-specific technologies used by manufacturers to configure and initialize hard drives, it is not always possible to 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 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 application 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 98. To modify the disk, do the following:

- Start your computer 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.

  For more information, see “About Rescue Disks” on page 39.

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

With your Norton Internet Security CD, you can create Emergency Disks. Although they are not as powerful as the Rescue Disks you create, you can use the Emergency Disks to recover from most common emergencies.

For more information, see “Creating Emergency Disks” on page 22.

You can use the CD that contains Norton Internet Security as an Emergency Disk if your computer can start from the CD-ROM drive.

For more information, see “Using the CD as an Emergency Disk” on page 116.

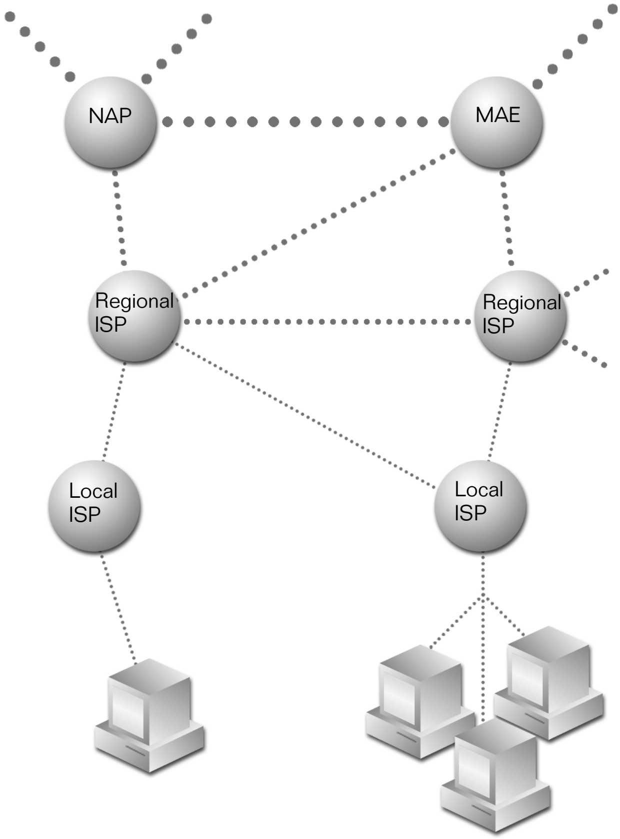
Once you have created the Emergency Disks, use them to solve the problem.

For more information, see “Using Emergency Disks” on page 116.

APPENDIX A

About the Internet

The Internet is the interconnection of millions of computers throughout the world. It comprises the computers and the connections that make it possible for any computer on the Internet to communicate with any other computer on the Internet.



The Internet is analogous to a system of roads and highways. The superhighways of the Internet, called the Internet backbone, carry large amounts of information over long distances. There are interchanges on the backbone, called network access points (NAPs) and metropolitan area exchanges (MAEs). There are regional highways provided by large Internet service providers (ISPs) and local streets provided by local ISPs.

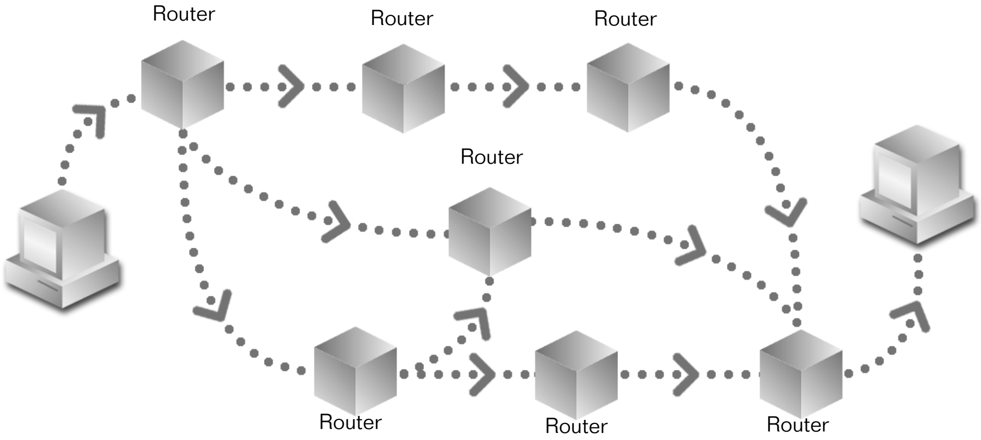
Like a system of roads and highways, the Internet provides multiple routes from one point to another. If one part of the Internet has too much traffic, or is damaged, information is rerouted to take a different route.

How information is transmitted over the Internet

All information sent across the Internet is communicated using a protocol called TCP/IP. Because all of the computers on the Internet understand this protocol, each one can communicate with every other computer on the Internet. TCP and IP are separate parts of this protocol.

The Internet is a *packet switched network*. Every communication is broken into packets by TCP (Transmission Control Protocol). Each packet contains the address of the sending and receiving computers along with the information to be communicated.

IP (Internet Protocol) is responsible for *routing* the packets to their destinations. Each packet may take a different route across the Internet, and packets may be broken up into *fragments*. Packets travel across the Internet, moving from one *router* to another. Routers look at the destination address and forward the packet to the next router. IP does not guarantee the delivery of every packet.



On the destination computer, TCP joins the packets into the complete communication. TCP may have to reorder the packets if they are received out of order, and it may have to reassemble fragmented packets. TCP requests retransmission of missing packets.

TCP/IP

TCP/IP is often used to refer to a group of protocols used on the Internet, including UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), and IGMP (Internet Group Membership Protocol).

UDP

UDP (User Datagram Protocol) is used for functions in which the reliability of TCP is not necessary, such as broadcasting video to multiple computers at once. UDP doesn't provide error correction or retransmission of lost packets.

UDP is secondary in importance to TCP when you browse the Internet.

ICMP

ICMP (Internet Control Message Protocol) packets contain error and control information. They are used to announce network errors, network congestion, timeouts, and to assist in troubleshooting.

Norton Internet Security normally allows certain inbound ICMP packets that provide you with information and are a minimal security risk. You can create rules to block some or all ICMP packets.

IGMP

IGMP (Internet Group Membership Protocol) is used to establish memberships in multicast groups. Your computer reports to a nearby router that it wants to receive messages addressed to a specific multicast group.

IGMP does not present a major security risk, but Norton Internet Security allows you to block the protocol entirely. This is a good idea if you do not use any applications that require IGMP. If you have problems receiving multicast information, such as movies or PowerPoint presentations, be sure that IGMP is not blocked.

Web information is located on the Internet

Web information is stored as pages, each with a unique name called a URL (Uniform Resource Locator).

When you enter a Web address in the browser address bar or click a link in your Web browser to move to a new Web site, you are giving your browser the URL of the page that you want to view. For example, www.symantec.com is a typical URL.

Each URL maps to the IP address of the computer that stores the Web page. URLs are used because they are easier to remember and type than IP addresses.

Before your browser requests a page, it asks a DNS (Domain Name System) server for the IP address of the Web site. IP addresses are 32-bit numbers expressed as four decimal numbers, each ranging from 0 to 255, and separated by periods: 206.204.104.148. Every computer on the Internet has a unique IP address.

Requesting a page

Once the browser has the IP address, it establishes a TCP *connection* to the Web server and requests the page. Each page that you view requires a new connection with the Web server. In fact, most pages require multiple connections, since each graphic (as well as many other page elements) requires its own connection.

Once a page is loaded, all of the connections are dropped. The process starts over for each page on the site, though your browser does remember the site's IP address.

Some newer Web sites that use HTTP 1.1 (Hypertext Transfer Protocol version 1.1) establish connections that can pass multiple files and stay open for multiple pages with a single connection.

Parts of a URL

A typical URL looks like this: http://www.symantec.com/securitycheck/index.html. Because you might want to block some parts of a domain, while allowing other parts of the same domain, you should understand what comprises a URL.

http://

The *application protocol* used to make the connection. The most common protocol for browsing the Web is http. Your browser assumes this is the application protocol if you don't enter one. Other commonly used protocols include ftp, and gopher.

.com

The *root domain* or *top-level domain*. There are several familiar root domains, including .com, .net, .edu, .org, .mil, and .gov. There are also two-letter root domains for most countries, such as .ca for Canada and .uk for United Kingdom.

symantec.com

The *domain*. This is the domain with which the browser establishes a connection. A domain frequently refers to a single company or organization that might have multiple Web sites on the Internet.

www.symantec.com

The *host*. This is the particular Web site with which the browser communicates. It is also the name for which DNS provides an IP address.

securitycheck	The *folder* or directory that contains the file to be accessed.
index.html	The *file name* of the file to be accessed.

There is one particular URL that identifies your computer to itself, and that is *localhost*. If you have a Web server on your computer, you can type http://localhost and see your Web page. The IP address that corresponds to localhost is 127.0.0.1.

Ports identify applications on a server

Ports, also called *sockets*, provide the location of a particular application or server on the remote computer with which you are trying to establish communication. This makes it possible to run multiple servers on a single computer. For example, many computers on the Internet run both a Web server and an FTP (File Transfer Protocol) server. The Web server uses port 80, while the FTP server uses port 21.

The terms *server* and *service* are used somewhat interchangeably. For example, a Web server provides the HTTP service, while it is usually said that a computer has the *Finger* service running.

Ports are numbered 1 through 65535. Ports 1 through 1023 are known as *well known ports* and are the default ports for many common Internet applications.

Ports are a part of the URL that is rarely seen. The port number follows the host name and a colon. For example:

http://www.symantec.com:80/securitycheck/index.html

Because the most-used ports are standardized, you rarely see port numbers. For example, Web browsers almost always use port 80, so they don't require that you type it unless you need to use a different port.

Well known ports

Some of the most common well known ports are:

Default port	Service name	Application
20	ftp-data	FTP (File Transfer Protocol) data
21	ftp	FTP (File Transfer Protocol) control
23	telnet	Telnet terminal handler
25	smtp	SMTP (Simple Mail Transfer Protocol)
53	domain	DNS (Domain Name Service) lookup
79	finger	Finger
80	http	HTTP (Hypertext Transfer Protocol)
110	pop3	POP3 (Post Office Protocol 3)
113	auth	Ident Authentication Service
119	nntp	NNTP (Network News Transfer Protocol)
137	nbname	NetBIOS name (Microsoft Networking)
138	nbdatagram	NetBIOS datagram (Microsoft Networking)
139	nbsession	NetBIOS session (Microsoft Networking)
143	imap	IMAP (Internet Message Access Protocol)
194	irc	IRC (Internet Relay Chat)
389	ldap	LDAP (Lightweight Directory Access Protocol)
443	https	HTTPS (Secure HTTP)

How computers are identified on the Internet

Millions of computers are connected to the Internet. When you are trying to identify computers, it is easier to work with groups of computers rather than having to identify each one individually. *Subnet masks* provide a way to identify a group of related computers, such as those on your local network.

A typical subnet mask looks like this: 255.255.255.0. At its simplest, each 255 indicates parts of the IP address that are the same for all computers within the subnet, while the 0s indicate parts of the IP address that are different.

Subnet masks are always used in conjunction with a base IP address.

For example:

Base IP address:	10.0.0.1
Subnet mask:	255.255.255.0

In this example, the range of IP addresses that the base IP address and subnet mask identify range from 10.0.0.1 to 10.0.0.255. The most common subnet mask used is 255.255.255.0 because it identifies a relatively small group of IP addresses, up to 254 computers. It is commonly used for very small groups of computers, including groups as small as two computers.

APPENDIX B

Understanding Internet risks

Norton Internet Security protects you from the major risks associated with the Internet. Those risks include the threat of hacker attack, malicious code in active content, exposure to inappropriate content, exposure of private information, and getting viruses from infected files.

Risks from hackers

The word *hacker* originally meant someone who could solve computer problems and write computer programs quickly and elegantly. However, the meaning of the term has changed to mean someone who uses his or her computer knowledge for illicit purposes. Since hacker started out as a complimentary term, some people use the word *cracker* for the derogatory form. In this text, hacker is used in its current, non-complimentary meaning.

You might also hear other terms for hackers, including *script-kiddies*, *wannabes*, *packet monkeys* and *cyberpunks*. These are all terms for hackers-in-training that use applications written by others (more advanced hackers) to attack computers on the Internet.

The process of a hacker attack

Most hacker attacks use the following process:

- Information gathering: The hacker gathers as much information about your computer as possible. The hacker attempts to find vulnerabilities without letting you know that your computer is under attack.
- Initial access: The hacker exploits a vulnerability found during information gathering and establishes an entry point into your computer.
- Privilege escalation: The hacker gains access to more of your computer.
- Covering tracks: The hacker hides or removes evidence of the visit, sometimes leaving a doorway open for return.

Information gathering

The first step in information gathering is acquiring a target. A hacker can choose a person or company to attack, or search the Internet for an unprotected target that will be easy to hack. The amount of information available about you on the Internet is directly related to your level of Web presence. If you have a domain name and a Web site, a lot more information is publicly available than would be if you only have an email address.

If a hacker has chosen a specific target, such as a company or organization, many resources on the Internet assist in gathering information. Most of them have legitimate uses, such as InterNic, which provides the Whois database of registered domain names. There are integrated tools, such as Sam Spade, which provides more than 20 different tools for finding and analyzing Internet information.

Using these tools, a hacker can learn a lot about a potential target. Given a domain name, it’s easy to use the Whois database to find out the name and address of the owner, as well as the name and phone number of the administrative and technical contacts. While this information usually can’t be used directly to attack a network or computer, it can be used to gather more information. It’s much easier to call a company, impersonate a network administrator, and ask a user for a password than it is to attack the network.

If a hacker doesn't have a specific target in mind, many tools are available for scanning the Internet and finding possible targets. The simplest scan is a *ping* scan, which can quickly scan thousands of computers. The hacker uses a program to ping computers at a series of IP addresses. Responses tell the hacker that a computer exists at that IP address. When Norton Internet Security is running, your computer is hidden from ping scans because your computer does not respond. The hacker does not learn that there is a computer at your IP address by pinging it.

Port scans are more comprehensive, usually performed on a single computer. A port scan can tell a hacker what services are running, such as HTTP and FTP. Each service that is running provides a potential entry point for the hacker. On unprotected computers, unused ports respond that they are closed, thus telling the hacker that a computer exists at that IP address. Norton Internet Security does not respond to scans of unused ports, giving them a *stealth* appearance.

Initial access

The easiest way for a hacker to access a Windows computer is to use Microsoft networking. On many computers, Microsoft networking is enabled so that anyone on the network can connect to it.

Microsoft's NetBIOS networking uses three of the Well Known Ports. These ports are used to establish connections between computers on a Microsoft network. In fact, they normally advertise the name of your computer over the local network. This is what you want on your own network, but it is not what you want on the Internet. Norton Internet Security is preset to block these ports and prevent someone on the Internet from connecting to your computer using Microsoft networking. If your computer is connected to a local network as well as to the Internet, you must change some settings to allow communication with the other computers on your network. Norton Internet Security still protects you from Internet risks while allowing you to use your local network.

For more information, see "Well known ports" on page 149.

For more information, see "Using Norton Internet Security on a home network" on page 126.

Privilege escalation

Once a hacker has connected to your computer, the next step is to gain as much control as possible. The steps involved and the results obtained vary greatly depending on the version of Windows running on the target computer.

On computers running Windows 95, Windows 98, or Windows Me, once a hacker has gained access to the computer, there is no need for escalation. They have full control of the computer. Luckily, these versions of Windows don't have much in the way of remote control features, so they are relatively easy to protect.

On computers running Windows NT or Windows 2000, the hacker will attempt to gain administrative rights to the computer. The key to getting administrative rights is usually a password. Instead of guessing, the hacker can download your password file and crack it.

Another tactic is to place a *Trojan horse* program on your computer. If a hacker can place a program such as Back Orifice, Subseven, or NetBus on your computer and get it running, it is possible to take control of the computer.

Other Trojan horse programs might record all your keystrokes to capture passwords and other sensitive data. Norton Internet Security and Norton AntiVirus provide two levels of protection against Trojan horse programs. Norton AntiVirus protects you from inadvertently running these programs. Norton Internet Security blocks the ports that Remote Access Trojan horse programs use to communicate over the Internet.

Covering tracks

When a hacker has gained as much control of a computer as possible, the task turns to concealing the evidence. As long as you don't know that a hacker has compromised your computer, you won't take steps to stop such actions.

On Windows NT and Windows 2000, hackers will try to turn off auditing and modify or clear the event logs. On any computer, the hacker may hide files so they are available for future visits. In extreme cases, a hacker might format the hard drive of a compromised computer to avoid identification.

Risks from active content

ActiveX controls and Java applets are called *active content* because they can do more than display text or graphics. Most active content is safe. Common uses of active content are pop-up menus and up-to-date stock quotes.

Both ActiveX and Java are supposed to be safe to run in your browser. ActiveX uses a system of digital certificates that lets you decide if you want an ActiveX control to run. Digital certificates appear as dialog boxes that ask if you want to install and run a control that appears when you are browsing the Web.

There are several problems with this system of using digital certificates. Some controls do not have certificates, and some certificates provide very little information about what the control does.

Java was originally designed to be safe to run in a browser. The Java *sandbox* was designed to prevent Java applets from reaching outside the browser to do anything that might harm your computer. However, hackers and security experts continually find ways to get around Java's safeguards and use Java's features in ways not conceived of by its developers.

Norton Internet Security monitors active content and can block all active content or warn you whenever active content is encountered. Norton AntiVirus Auto-Protect detects malicious ActiveX controls and prevents them from running.

Risks from inappropriate content and activities

There is a wealth of information on the Internet that is easily accessible to all. However, some topics may not be suitable for children. For example, most people consider pornography and intolerance sites to be inappropriate for children to view. You may feel that other sites should also be off limits for your children.

Blocking site categories

Norton Internet Security lets you choose the categories of sites that you want to prevent your children from seeing. While Norton Internet Security has a frequently updated, categorized list of sites to be blocked, you can also add specific sites to the list. Because children have different needs at different ages, you can block different content for different users with Norton Internet Security accounts.

Restricting access to applications

Some Internet-enabled applications might also be inappropriate for children to use. For example, you may not want your children to use realtime chat applications. You may also want to restrict your children from using file transfer programs. This reduces the risk of inadvertent introduction of a virus, worm, zombie, Trojan horse, or other malicious code to your computer. It also protects the children from downloading pornography or pirated software.

Norton Internet Security lets you choose the categories of programs that your children are allowed to use. It keeps the list of programs up-to-date, so your protection stays current as new programs are released. You can also add custom applications, and you can control their use as well.

Risks to your privacy

The Internet presents several risks to your privacy. Some sites collect and save personal information, such as credit card numbers. Some sites track your Internet usage. Some applications send information about your computer usage to Web sites without your permission.

Sending confidential information

You probably don’t want confidential information, such as credit card numbers, or your home phone number, to be sent unencrypted over the Internet. Privacy Control prevents confidential information from being entered on Web sites that do not use secure, encrypted communications, and from being sent on instant messenger programs.

You may want to prevent some users in your household from ever sending confidential information over the Internet. Norton Internet Security can block a user from accessing secure sites where they might be asked for personal information.

Good cookies and bad cookies

Cookies are messages sent to your browser by a Web site and stored as small files on your computer. They are often used by Web sites to track your visits. In most cases, the cookie file does not contain any personal information, instead carrying only an identifier that identifies you to a Web site.

Good cookies

In their most benign form, cookies last only until you close your browser. This type of cookie is mainly used to help remember choices you have made as you navigate through a Web site.

Many sites leave cookies on your computer so that they recognize you when you return to their site. These cookies identify you so that options you have chosen in the past are used for your current visit to the site. If you frequent a site that remembers the stocks that you want to track, for example, it probably uses this kind of cookie.

Bad cookies

In one of their malevolent forms, cookies from one Web site might track your visits to a different Web site. For example, most of the ads that you see on Web sites do not come directly from the site that you are viewing, but from sites that provide ads to many different sites. When the advertising site displays the ad, it can access cookies on your computer. This allows the advertising company to track your Web usage over a broad range of sites and profile your browsing habits.

Blocking cookies

Norton Internet Security can block all cookies or it can notify you of each cookie request. If you block all cookies, you will lose functionality at many Web sites. For example, you might not be able to make purchases from some Internet stores. If you choose to be prompted each time a Web site tries to create a cookie, you can evaluate each request and block those that are not from the site that you are viewing. Norton Internet Security can block or allow cookies from particular domains or Web sites.

Tracking Internet use

As you browse the Internet, most browsers freely pass on several bits of information that you might want to keep confidential. One item that your browser normally passes to Web sites is the URL of the page from which you came. This information is used by some Web sites to help you navigate inside the Web site, but it can also be used to identify the Web site you came from. In other words, it can be used to track your Web usage. Norton Internet Security blocks this information.

Your browser also sends information about itself and the operating system that you are using. While Norton Internet Security can block this information, it is usually used by Web sites to provide Web pages that are appropriate to your browser.

A possibly more sinister invasion of your privacy is found in programs you install on your computer that, without your knowledge, report information back to a Web site. Several programs that help you download and install files have been discovered to report your activities across the Internet. Norton Internet Security protects your privacy by alerting you to these communications.

Risks from Trojan horses and viruses

Nowadays, with so many computers connected by networks and the Internet, viruses can spread more rapidly than they could in the days of *sneakernet*, when files were transferred from computer to computer on disks. Additionally, the risk has broadened from viruses to Trojan horses, *worms,* and *zombies*.

A virus is a program or code that replicates by attaching itself to another program, a boot sector, a partition sector, or a document that supports macros. Many viruses just replicate, but others do damage. A virus can arrive in a document that you receive by email.

A Trojan horse is a program that does not replicate, but damages or compromises the security of the computer. Typically, it relies on someone emailing it to you; it does not email itself. A Trojan horse may arrive disguised as useful software. Some Trojan horse programs do malicious things to the computer on which they are run, while others, such as Back Orifice, provide remote control capabilities for hackers.

A worm is a program that makes copies of itself—for example, from one disk drive to another, or by sending itself through email. It may do damage or compromise the security of the computer. A worm can arrive as an attachment to an email that has a subject that tempts you to open it.

A zombie program is a dormant program secretly implanted on a computer. Later, it is awakened to aid in a collective attack on another computer. Zombie programs don’t normally damage the computer on which they reside, but are used to attack other computers. A zombie program can arrive as an email attachment.

Norton AntiVirus protects you from receiving and executing viruses, Trojan horse programs, worms, and zombie programs. Norton AntiVirus scans email as you receive it from the Internet and also checks files as you access them with your computer. This gives you two levels of protection against these risks.

Norton Internet Security ensures that Trojan horse programs do not communicate over the Internet. This means that you are protected from hackers who use Trojan horse programs.

The likelihood of being attacked

The Internet presents many risks. What are the odds that your home computer will be the subject of an attack?

The chance of a hacker singling out your computer from all of those on the Internet is probably very slim. However, the use of these tools by neophyte hackers, or script kiddies, to find targets means that your computer will be scanned relatively frequently for vulnerabilities. The more vulnerabilities found, the more inviting your computer is to the hacker.

The tools that hackers use to find vulnerable targets can scan large groups of computers on the Internet. The hacker simply enters a range of IP addresses to be scanned and clicks OK. The program checks each IP address in the range to see if a computer is there. If it finds a computer, it performs a series of tests to identify vulnerabilities, such as having Microsoft networking enabled over the Internet. The hacker returns to find a list of computers and their vulnerabilities.

Norton Internet Security protects you from these scans by making your computer almost invisible. Your computer simply won't respond to the queries that these scanners send. This means that your computer will exhibit no vulnerabilities to the hacker, making it a poor target for attack.

SUPPORT

Service and support solutions

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

Technical support

Symantec offers several technical support options:

- Online Service and Support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. This gives you access to current hot topics, knowledge bases, file download pages, multimedia tutorials, contact options, and more.

- PriorityCare telephone support

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

  You can also access the PriorityCare number for your product through the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options available for your product and version.

- Automated fax retrieval

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

Support for old and discontinued versions

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

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

Customer service

Access customer service options through the Service & Support Web site at http://service.symantec.com. From this site, you can receive assistance with non-technical questions, and for information on how to do the following:

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

For upgrade orders, visit the online upgrade center at:
http://www.symantecstore.com

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under the Global Service and Support.

Service and support offices

North America

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

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

Automated Fax Retrieval

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

Argentina and Uruguay

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

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

Asia/Pacific Rim

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

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

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

Europe, Middle East, and Africa

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

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

Mexico

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

http://www.service.symantec.com/mx
+52 (5) 661-6120

Other Latin America

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

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

Subscription policy

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

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

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

July 13, 2001

Norton Internet Security™
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 distributer.

Briefly describe the problem:____

____

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

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

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ ________ __ Visa __ Mastercard __ American Express

Credit Card Number ____Expires _________

Name on Card (please print) ______________________________ Signature ______________________

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

MAIL YOUR CD REPLACEMENT ORDER TO:

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

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

symantec.™

INDEX