MCAFEE

Total Protection For Your PC

McAfee Guard Dog

User's Guide

COPYRIGHT

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES, INC. ("McAfee"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, McAfee hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, "smart phone" or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

   a. **Use.** The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all of the Software's proprietary notices.

   b. **Server Use.** You may use the Software on a Client Device as a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to, accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the Documentation's proprietary notices.

c. **Volume Licenses.** If the Software is licensed with volume license terms specified in the applicable price list or product packaging for the Software, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume license authorizes. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Documentation's proprietary notices.

2. **Term.** This Agreement is effective for an unlimited duration unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. **Updates.** For the time period specified in the applicable price list or product packaging for the Software you are entitled to download revisions or updates to the Software when and as McAfee publishes them via its electronic bulletin board system, website or through other online services. For a period of ninety (90) days from the date of the original purchase of the Software, you are entitled to download one (1) revision or upgrade to the Software when and as McAfee publishes it via its electronic bulletin board system, website or through other online services. After the specified time period, you have no further rights to receive any revisions or upgrades without purchase of a new license or annual upgrade plan to the Software.

4. **Ownership Rights.** The Software is protected by United States copyright laws and international treaty provisions. McAfee and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software and Documentation made hereunder must contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not rent, lease, loan or resell the Software. You may not permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement, except to the extent such use is specified in the applicable list price or product packaging for the Software. You may not transfer any of the rights granted to you under this Agreement. You may not reverse engineer, decompile, or disassemble the Software, except to the extent the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon, the Software in whole or in part. You may not copy the Software or Documentation except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by McAfee. McAfee reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

6. **Warranty and Disclaimer**

   a. **Limited Warranty.** McAfee warrants that for sixty (60) days from the date of original purchase the media (e.g., diskettes) on which the Software is contained will be free from defects in materials and workmanship.

   b. **Customer Remedies.** McAfee’s and its suppliers’ entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at McAfee’s option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained. You must return the defective media to McAfee at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent McAfee is subject to restrictions under United States export control laws and regulations.

   c. **Warranty Disclaimer.** Except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MCAFEE DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, MCAFEE MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL MCAFEE OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL MCAFEE BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE MCAFEE CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF MCAFEE SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

8. **United States Government.** The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. **Export Controls.** Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the United States Treasury Department’s list of Specially Designated Nations or the United States Commerce Department’s Table of Denial Orders. By downloading or using the Software you are agreeing to the foregoing and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list.

   IN ADDITION, YOU SHOULD BE AWARE OF THE FOLLOWING: EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE.

SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY PERSONAL OR BUSINESS USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION TO, OR IMPORTATION OF, ENCRYPTION BY: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE IT IS YOUR ULTIMATE RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS AND THAT MCAFEE HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

10. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). McAfee expressly disclaims any express or implied warranty of fitness for High Risk Activities.

11. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. This Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. This Agreement supersedes any other communications with respect to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee or a duly authorized representative of McAfee. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

12. **McAfee Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact McAfee for any other reason, please call (408) 988-3832, fax (408) 970-9727, or write: McAfee Software, 3965 Freedom Circle, Santa Clara, California 95054. http://www.mcafee.com.

Statements made to you in the course of this sale are subject to the Year 2000 Information and Readiness Disclosure Act (Public Law 105-271). In the case of a dispute, this Act may reduce your legal rights regarding the use of any statements regarding Year 2000 readiness, unless otherwise specified in your contract or tariff.

Table of Contents

Chapter 1. Welcome to Guard Dog™ 1

Guard Dog and the Internet 1

How Guard Dog works 1

Guard Dog and your Internet Connection 1

What Internet problems Guard Dog solves 2

What’s new in Guard Dog 3

About Guard Dog documentation 4

How this book is organized 5

Using Guard Dog help 5

Chapter 2. Installing Guard Dog™ 7

System requirements 7

Installing Guard Dog 8

Troubleshooting installation problems 9

Step 1: Clean up your hard drive 9

Step 2: Remove temporary files 10

Step 3: Close other software 11

Installing other software from the Guard Dog CD 11

Chapter 3. Quick Tour of Guard Dog™ 13

Viewing the Guard Dog video 13

Using the Guard Dog interview 13

What information does Guard Dog ask me to enter? 14

Why should I create an Emergency Disk? 15

How password protection effects using Guard Dog 16

Using the Guard Dog Home screen 17

Opening and closing the Guard Dog Home screen 18

Performing a CheckUp 19

Updating Guard Dog 20

Viewing the Log 20

What Guard Dog does while your PC is running 21

Using the Guard Dog shortcut menu 21

Responding to Guard Dog alert messages 22
Using Browser Buddy to retrieve or store your Web site passwords .23
Using file encryption 25

Chapter 4. Customizing Guard Dog™ 27
Restarting the Interview 27
Changing Protection Settings 27
Preferences settings 29
Scheduling Guard Dog actions 29
Changing CheckUp Settings 32

Chapter 5. Privacy Features 35
What Cookie Blocker does 35
Responding to a Cookie Blocker alert message 36
Why should I change my Cookie Blocker settings? 37
What Identity Protector does 37
Responding to an Identity Protector alert message 38
Why should I change my Identity Protector settings? 39
What Web Trail Cleaner does 39
Responding to the Web Trail Cleaner alert message 40
Why should I change my Web Trail Cleaner settings? 41
What Search Filter does 41

Chapter 6. Security Features 43
What Gatekeeper does 43
Responding to a Gatekeeper alert messages 43
Why should I change my Gatekeeper settings? 45
What File Guardian does 46
Responding to a File Guardian alert messages 47
Why should I change my File Guardian settings? 49
What Password Manager does 50

Chapter 7. Using AntiVirus Features 53
Looking for viruses with CheckUp 53
Continuing virus protection 53
What Virus Sentry does 54

Responding to a Virus Sentry alert message 54
Why should I change my Virus Sentry settings? 54
Keeping virus protection up-to-date 57
Appendix A. Internet Security and Privacy 59
Networks and the Internet 59
TCP/IP is the subsystem 59
Why packets? 60
The Internet and the Web…what is the difference? 60
Privacy and security on the Web 61
Why does Internet privacy matter to me? 61
Privacy on the Web 62
Who is snooping? 62
Snooping and sniffing 62
Web servers and firewalls 62
What can I do to keep my stuff safe? 63
How can I tell if a Web site is secure? 63
How does encryption work? 64
Security on the Web 65
Nasty applets 66
Can I prevent programs from accessing the Internet? 66
Computer viruses and the Web 66
Are viruses really that dangerous? 67
Types of viruses 67
How can my PC become infected with a virus? .68
Frequently asked questions about Internet privacy .68
Sources for Internet privacy and security information 70
Finding out about Internet hoaxes 70
More information about computer viruses 70
More information about security 71
More information about privacy 71
Appendix B. Product Support 73
How to Contact McAfee 73
Customer service 73

Technical support 74
McAfee training 74

Welcome to Guard Dog™ 1

Guard Dog and the Internet

In the last few years the Internet has changed from a communications network used almost exclusively by governments and universities to an information treasure house used by people of all ages and occupations. With an Internet account you can send electronic mail (e-mail) around the world in seconds, do research without leaving home, meet new friends in an online chat room, or shop without getting out of your bathrobe. However, with all this potential comes a certain element of risk. When you use the Internet, information is transmitted from your computer to other computers in the Internet—information you may not want people to have. And those computers can also send files to your computer. While most of these files are harmless, some can invade your privacy or even damage the data on your computer's hard drive.

How Guard Dog works

There are two main ways that Guard Dog protects you:

- You can find any potential privacy, security, and virus threats that exist on your PC by performing a CheckUp. You are guided step-by-step through solving each problem.
- Once installed, a portion of Guard Dog remains active in your PC's memory and watches over your PC. When Guard Dog detects a potential problem, it takes action based on your preferences—it either takes care of the problem automatically or pops up an alert message to ask you how to proceed.

With Guard Dog, you are in control at all times. You decide what security and privacy features to use. If your concerns or computing habits change, it is easy to change Guard Dog to meet your needs.

Guard Dog and your Internet Connection

Guard Dog relies on your Internet Connection to provide its Internet security features. Unless you have an Internet provider and browser software designed for Windows 95 or Windows 98, Guard Dog can provide only virus protection.

To use all Guard Dog features, you must have an Internet connection through a local network or a modem. Some networks have an Internet connection that you can use by connecting to the network-either directly or through dial-up networking. If you don’t connect through a network, your computer must have a modem installed.

You can establish an Internet connection through an Internet Service Provider (ISP) such as Netcom or Earthlink. An ISP acts as a middleman between you and the Internet Your computer connects (using your modem) to the ISP’s equipment, which in turn connects to the Internet. You may also be connected to the Internet through an online service such as America Online or Compuserve.

In addition, you must also have a browser. A browser is software, such as Netscape Navigator or Microsoft Internet Explorer (it must be a version designed for Windows 95 or Windows 98), that allows you to view text and graphics and download files from Web sites. America Online 3.0 for Windows 95 and Compuserve Interactive 3.0 both include browsers that are compatible with Guard Dog.

What Internet problems Guard Dog solves

This section briefly describes how Guard Dog protects you from the most common Internet threats. If you want more background information on Internet privacy, security, and virus issues, see “Internet Security and Privacy” on page 59.

Privacy threats

- **Identity Protector** monitors your Internet connection and warns you before private information is sent to an unsecure Internet site. It stops programs and other people that use your computer (like your kids) from sending your name and credit card numbers over the Internet without your OK.

- **Cookie Blocker** prevents Web sites from storing cookies on your hard drive. Third-party Web sites use cookies to track your Web browsing habits. You can choose your level of interaction with Cookie Blocker. (For more information, see “What are cookies and how are they used?” on page 69.)

- **Web Trail Cleaner** cleans up your Web browsing trails—cached files, list of URLs (*Uniform Resource Locator*, also known as Web address) visited, history file—when you close your browser. Others can track your online movements by viewing the files and URLs left over from your Internet browsing.

- **Search Filter** prevents search information that you request at one Web site from being passed along to the next site you visit. Without Search Filter, your browser can transfer your search request information from one Web site to another without your knowledge.

Security threats

- **Gatekeeper** lets you control the programs that have access to your Internet connection. Programs on your PC can be programmed to access to the Internet without your consent.
- **CheckUp** can check for and if necessary, display the Web page from which you can install the latest Netscape or Internet Explorer version. Older Netscape or Internet Explorer software installed on your PC may have security flaws.
- **File Guardian** protects files that contain your sensitive data from being opened, renamed, copied, moved, or deleted. Programs, such as ActiveX and Java programs, can scan your PC for personal information or delete files without your permission.

  File Guardian also limits access to protected files either to programs you specify or through file encryption. It can limit the programs that can access your tax, on-line banking, or personal accounting data files.
- **Password Manager** stores your Web site login names and passwords for protected Web sites in one secure location. When you are visiting a site that requires this information, drag it from Browser Buddy to the form displayed in your browser. No more storing your login names and passwords in an unsecure location, such as on a sticky note on your monitor or in a text file on your Windows desktop.

Virus threats

- **Virus Sentry** checks for boot sector, partition table, and memory viruses during your DOS startup. It also watches for viruses while you work with program, document, and e-mail attachment files.
- **Virus Check** in either CheckUp or Scheduler will catch file and macro viruses, and Trojan Horses.

What’s new in Guard Dog

Guard Dog version 2 includes these new features.

- **New interface**
  Easier to use—you don’t have to know a lot about the inner workings of your PC and the Internet.
- **Guard Dog password**
  Protects the information and settings in Guard Dog from being viewed or changed. It also prevents others using your computer from sending out information that you specify as private.
- **Multimedia introduction tutorial**
  Walks you through Guard Dog’s features and teaches you the facts about today’s Internet threats.
- **Improved cookie management**
  Selectively remove cookies that you don’t want in CheckUp.
- **Personal identity protection**
  “Mark” personal identity information and sensitive files (such as financial records and credit card numbers) so they’ll never be sent over the Internet without your OK.
- **Additional Scheduled events**
  Schedule events that automatically:
  - Remove viruses and other hostile programs.
  - Remove cookies, browser History records, and browser Cache files.
  - Encrypt or decrypt files protected by File Guardian.
  - Remind you to create or update your Emergency Disk or Guard Dog files.
- **Encrypt sensitive files**
  Add an extra layer of protection by encoding files to prevent them from being read—until you decode them.
- **Web site password management**
  Store and manage your Web site passwords in one convenient, secure location.

About Guard Dog documentation

This manual provides the basic information you need to install, set up, and use Guard Dog. More detailed information about Guard Dog is provided by Help.

How this book is organized

This User's Guide is designed to get you using Guard Dog quickly. Read chapters 1 and 2 to get Guard Dog installed and running. You need only read Chapters 3, 4, 5, and 6 if you want further information on customizing Guard Dog or using specific features. If you are new to the Internet or just want to find out more about Internet privacy and security issues, read Appendix A.

Table 1-1.

To find out	Read
What this version of Guard Dog does and how to find information about Guard Dog.	Welcome to Guard Dog™
System requirements and how to install Guard Dog.	Chapter 1. Installing Guard Dog™
How to use the main features of Guard Dog.	Chapter 2. Quick Tour of Guard Dog™
How to change CheckUp and Protection settings or schedule automatic checks and reminders.	Chapter 3. Customizing Guard Dog™
What the Cookie Blocker, Identity Protector, Web Trail Cleaner, and Search Filter features are and how to work with them.	Chapter 4. Using Guard Dog Privacy Features
What the Gatekeeper, File Guardian, and Password Manager features are and how to work with them.	Chapter 5. Using Guard Dog Security Features
What the AntiVirus features are and how to work with them.	Chapter 6. Using Guard Dog AntiVirus Features
What privacy, security, and virus issues exist on the Internet.	Appendix A. About Internet Security and Privacy
How to contact McAfee Software sales, customer service and support departments.	Appendix B. Contacting McAfee Software

Using Guard Dog help

To view Guard Dog

1. In the Guard Dog Home screen, click Help.
2. Click Contents and Index to open the Help Topics window.

3. Click one of the following:
   - Contents displays the topics in the Help file organized in book form.
   - Index lets you search for specific information.

To display help for a screen

1. In the Guard Dog Home screen, click Help.
2. Click Help for this screen to display a help topic that explains what you can do in or what you may need to know about the current Guard Dog screen.

To get help for settings in a dialog box

- Whenever you see the ? button in the upper-right corner of a dialog box, click the button, then click on the setting for which you want information.

Installing Guard Dog™ 2

Most installation problems are a caused by having programs running while you try to install new software. Even if the installation appears normal, you won't be able to run the new program. To avoid installation problems, close all open programs before you install Guard Dog, including programs that run in the background, such as screen savers or virus checkers.

System requirements

To use Guard Dog you need:

- IBM PC or compatible computer running Windows 95 or Windows 98.
- 16 megabytes (MB) minimum of RAM.
- 20 MB free hard disk space to install Guard Dog and Oil Change. Additional disk space is required to install any optional Internet software that may be included on the compact disc (CD) version.
- 256-color video display or better. Guard Dog looks and operates best in a resolution of 800x600 pixels (or greater) and a color palette of 32,000 color mode (15 bit) or higher. 256-color palette is supported, but may cause some color changes (caused by 'palette swapping') when switching between applications.
- Microsoft mouse or compatible pointing device.
- Access to the Internet, either a dial-up account with an Internet Service Provider (ISP) or a constant connection through a network.
- Sound card (not required, but you'll need this to hear the sound for the Guard Dog video).
- Windows 95 Web browser (also called a 32-bit browser).

  Some Help features—McAfee Software on the Web, Guard Dog on the Web, FAQs, and Report a problem—require you to connect to the McAfee Software Web site with a Web browser (software that allows you to view documents and download files from the World Wide Web). To use all the online support features, the browser must be Microsoft® Internet Explorer, Netscape Navigator™, or America Online v3.0 (or later) for Windows 95.

NOTE: America Online users need AOL's 32-bit Winsock to use Guard Dog. To upgrade from a 16-bit Winsock, contact America Online.

Installing Guard Dog

After closing all open programs, you are ready to install Guard Dog on your PC. Installation should go smoothly, however, if you do have difficulties, see "Troubleshooting installation problems" on page 9.

To install Guard Dog

1. Close all open programs.
2. Insert the Guard Dog CD in the CD-ROM drive.
3. In the Guard Dog Setup screen, click Install Guard Dog.

   NOTE: If the setup screen doesn't start automatically when you close your CD-ROM drive, click Start on the Windows taskbar, click Run, then type d:\setup. If D is not the drive letter of your CD-ROM drive, substitute the correct drive letter.

4. Read the text in the Welcome to Guard Dog screen, then click Next to display the Software License Agreement.
5. After you read the license agreement, click Yes to continue.
6. In the Choose Destination Location window, do one of the following:
   - To install the software into the default location C:\Program Files\Guard Dog, click Next>.
   - To install the files in an alternate location, click Browse, locate the appropriate directory, and then click OK. Click Next> to copy the Guard Dog files to your hard drive.
7. After the Guard Dog files are copied to your PC, you are asked if you want to register Guard Dog over the Internet. To register, click Yes.

   The McAfee Software Online Registration wizard steps you through the registration process. Online registration is optional. If you do not register Guard Dog during installation, you can do so later from the Start menu by choosing Register Guard Dog from the Guard Dog menu.

8. After registration, you are asked if you want to install a limited subscription version of McAfee Software Oil Change™. To use Guard Dog's Update feature, you must have Oil Change installed. Do one of the following:

    - Click Yes to install Oil Change (with a limited subscription).

    - Click No to install Oil Change later from the Guard Dog CD. For more information, see "Installing other software from the Guard Dog CD" on page 11.

9. The final installation screen notifies you that the installation is complete and lets you choose to view the Guard Dog ReadMe file and start Guard Dog. (You should read the ReadMe file, as it contains information that isn't included in this manual.) By default, these options are selected. To disable either option, clear its check box. Click Finish.

10. The Readme file and a message that asks permission to restart your PC appears. Do the following:

    - Click the Readme window to read the file. Close the window when you are finished.

    - Click Yes in the message box to restart your PC. Guard Dog can't begin monitoring your PC until you do so.

      After you restart your computer, Guard Dog opens automatically, plays its introductory video, and then starts its interview. For more information, see "Viewing the Guard Dog video" on page 13 and "Using the Guard Dog interview" on page 13.

Troubleshooting installation problems

A failed installation can cause software problems that are difficult to track down. The major causes of installation failure are:

- Hard drive errors

- Temporary files that conflict with the installation

- Attempting to install while other software is running

Follow the procedure outlined below to minimize the affect that these common conditions may have on your installation.

Step 1: Clean up your hard drive

Run the Windows 95 hard drive utilities, ScanDisk and Disk Defragmenter to identify and fix any errors on your hard drive:

1. Click Start on the Windows taskbar, point to Programs, then Accessories, then System Tools, and click ScanDisk.
2. In the ScanDisk window, select Standard and Automatically fix errors (these are the default settings).
3. Click Advanced. In the Advanced Settings dialog box, make sure the following settings are selected:
   - Only if errors found
   - Replace log
   - Delete
   - Free
4. Ignore the other options, and click OK. Click Start. ScanDisk begins scanning your drive for errors. Depending on the size of your hard drive, ScanDisk may take several minutes to complete its job.
5. When ScanDisk is finished, close ScanDisk.
6. Click Start on the Windows taskbar, point to Programs, then Accessories, then System Tools, and click Disk Defragmenter.
7. Click OK to start Disk Defragmenter. Depending on the speed of your computer and the size of your drive, this may take several minutes to complete.
8. Close Disk Defragmenter when it has finished defragmenting your disk.

Step 2: Remove temporary files

Delete the contents of the Windows Temp folder:

1. Double-click the My Computer icon on your desktop. The My Computer window opens. Double-click the C: drive. You are now viewing the contents of your hard drive.
2. Double-click the Windows folder.
3. In the Windows folder, double-click the Temp folder.
4. In the menu, click Edit, then click Select All. All of the items in your Temp folder are now selected.
5. Press the Delete key on your keyboard to delete the files. If Windows asks about deleting files, click Yes.
6. In the Windows taskbar, click Start, then click Shut Down.

7. Click Restart the computer, then click Yes in the Shut Down Windows dialog box to restart your PC.

Step 3: Close other software

Disable all software running in the background:

1. Hold down the Ctrl and Alt keys on your keyboard, and then press the Delete key once. The Close Program dialog box appears.
2. Click End Task for every item on the list except Explorer.
3. Repeat steps 2 and 3 until you've closed everything except Explorer.
4. When you see only Explorer in the Close Program dialog box, click Cancel.

   You are now ready to install your new software.

Installing other software from the Guard Dog CD

The Guard Dog CD may contain additional Internet programs or trial copies of other McAfee Software products.

To install optional software

1. Insert the Guard Dog CD in the CD-ROM drive.
2. In the Guard Dog Setup screen, click Other Software Products.
3. Follow the instructions on your screen.

Quick Tour of Guard Dog™ 3

Guard Dog is a simple program to use. In fact, this one chapter covers the main things you need to know about using Guard Dog. You begin by watching the Guard Dog video, after which you must answer a few questions so that Guard Dog can effectively protect the sensitive data on your PC.

Viewing the Guard Dog video

After you install Guard Dog and restart your computer, Guard Dog plays its video. The video introduces you to Internet privacy and security issues and guides you through Guard Dog's main features.

If you want to stop the video before it is done playing, press the Esc key. If you want to view the video again, click Help on the Guard Dog Home screen, then click How Guard Dog works.

After the video finishes playing, Guard Dog displays its interview.

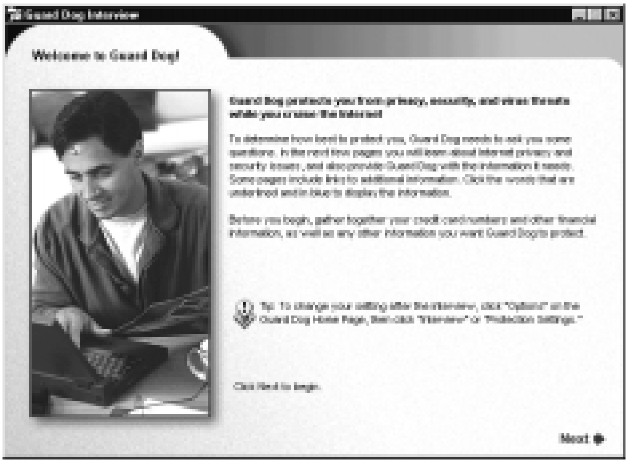
Using the Guard Dog interview

The interview starts automatically after the Guard Dog video finishes playing for the first time. Although Guard Dog is set up to use security, privacy, and virus settings that are appropriate for most users, some features require your input. The interview provides an easy means of customizing your Guard Dog settings.

To rerun the interview at a later time, click Interview in the Options menu on the Guard Dog Home screen.

Each interview screen either tells you about a Guard Dog feature, asks you to enter information, or asks you how you want Guard Dog to respond to certain situations. (Figure 3-1.)

Figure 3-1. Guard Dog Interview screen.



Guard Dog protects you from privacy, security, and virus threats while you cruise the Internet

To determine how best to protect you, Guard Dog needs to ask you some questions. In the next few pages you will learn about Internet privacy and security issues, and also provide Guard Dog with the information it needs. Some pages include links to additional information. Click the words that are underlined and in blue to display the information.

Before you begin, gather together your credit card numbers and other financial information, as well as any other information you want Guard Dog to protect.

Tip: To change your setting after the interview, click "Options" on the Guard Dog Home Page, then click "Interview" or "Protection Settings."

Click Next to begin.

On each interview screen you can click Back to return to a previous screen or click Next to move to the next screen. In the final interview screen, you click Finish to save the settings you selected and close the interview.

What information does Guard Dog ask me to enter?

The Guard Dog interview asks you to enter the personal and financial information that you want to protect. All the information you enter into Guard Dog is stored in encrypted form on your hard disk—it is never sent to McAfee Software.

You may want to gather your personal information before you start the interview. If you don't have the information readily available or if you change your mind, you can rerun the interview or add information directly using Protection Settings. Guard Dog asks you to enter:

- A password that you use to protect your Guard Dog information.
- Personal and financial information that you want to protect from being sent out over the Internet:
  - Name
  - Address

  - Social Security number
  - Telephone number
  - E-mail address
  - Other financial numbers such as bank account, brokerage account, credit card, phone card, and so on.
- Any Web site login names and passwords that you want to store in Password Manager.
- For optimal protection by Identity Protector, include all dashes (such as Social Security number, bank account numbers, brokerage accounts, and ATM cards). For example, if you enter 123-45-6789 as your social security number, Guard Dog will recognize the number with or without the dashes. If you enter 123456789, Guard Dog won't alert you if the number is sent out with dashes (123-45-6789). Credit cards do not need dashes because you type the numbers into separate boxes.

> **NOTE:** You can fine-tune the configuration of Guard Dog's privacy, security, and AntiVirus features in Protection Settings. Click **Options** on the Guard Dog Home screen, then click **Protection Settings**.

Why should I create an Emergency Disk?

As part of the interview, Guard Dog asks you to create an Emergency Disk. The Emergency Disk saves critical information and files that can be used to start up (or *boot*) your computer when it can't start normally. If you should encounter a boot sector virus, you may need the Emergency Disk in order to start up your computer and clean the virus.

If you think that your computer is in good condition, now is the best time to create an Emergency Disk. You will need three formatted, high-density, 3.5-inch floppy disks. (If you need help formatting the disks, refer to Windows Help, which is located on your Windows **Start** menu.)

In case anything should happen to your installed copy of Guard Dog, the Emergency Disk also contains a copy of your Guard Dog settings (including the Guard Dog password) and Password Manager information. Keep your Emergency Disk in a secure location away from heat and magnetic surfaces.

If you choose not to create an Emergency Disk at this time, you can create one later by running CheckUp. Guard Dog also reminds you every four months to create or update your Emergency Disk. You can also create an Emergency Disk by running the Interview and clicking Next until you reach the Emergency Disk page.

How password protection effects using Guard Dog

If you set up Guard Dog to use a password—either through the Interview or Preferences in Protection Settings—you are prompted for the Guard Dog password when you start Windows. When you enter an incorrect password, Guard Dog displays the hint that you provided when you created your password.

Without the password you can still open the Guard Dog Home screen, but you won't be able to change your CheckUp Settings or Protections Settings. Also, Guard Dog won't let you use the Password Manager information in Browser Buddy or send out information protected by Identity Protector.

If you've forgotten your Guard Dog password, you can retrieve it from the Emergency Disk, so remember to keep your disks in a secure location.

WARNING: If you forget your password and didn't create an Emergency Disk, you can reinstall Guard Dog to use it—but you'll lose your Guard Dog settings, Password Manager information and won't be able to use any of your encrypted files.

To retrieve your Guard Dog password

1. When you try to use a Guard Dog password-protected feature, the Guard Dog Password dialog box appears. In the dialog box, click OK. The Guard Dog Login Failed dialog box appears.
2. Insert the first disk of your Emergency Disk set into your floppy disk drive and click Browse.
3. Click the icon for your floppy drive and click OK.

TIP: Use Interview when you want to change your Guard Dog password, then update your Emergency Disk set (you can reuse the same disks) to store your changed password information.

Using the Guard Dog Home screen

After the interview ends, Guard Dog displays its Home screen (Figure 3-2).

Figure 3-2. Guard Dog Home screen.

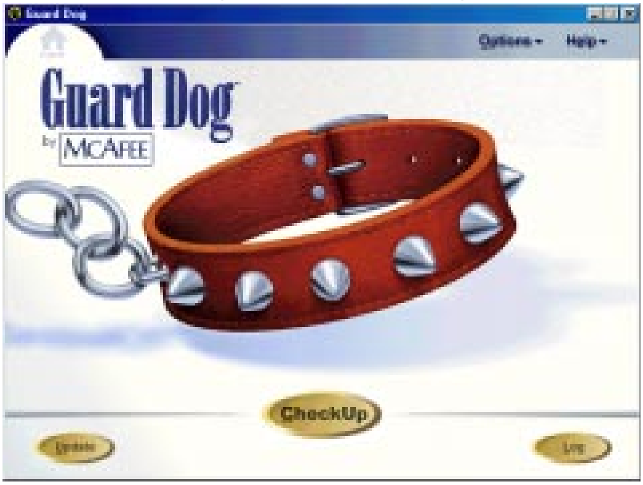


Table 3-1. Actions you can perform in the Home screen

To do this	Click this
Run a complete check of your PC for privacy, security, and virus problems.	CheckUp
Adjust the CheckUp settings.	Options, then click CheckUp Settings
Adjust the Guard Dog general or alert settings.	Options, then click Protection Settings
Display a list of Guard Dog actions.	Log
Display the McAfee Software Home screen in your Web browser.	Help, then McAfee Software on the Web
Display the McAfee Software Support page in your Web browser.	Help, then Guard Dog on the Web
Display the Support FAQ page in your Web browser.	Help, then Frequently Asked Questions
Create an e-mail message addressed to McAfee Software Technical Support site.	Help, then Report a problem

Table 3-1. Actions you can perform in the Home screen (Continued)

To do this	Click this
Launch the Guard Dog help file.	Help, then either Contents and Index or Help for this screen
Display your Guard Dog version number.	Help, then About
Read virus descriptions.	Help, then Virus Encyclopedia
Close the Guard Dog Home screen. (This doesn’t affect the monitoring portion of Guard Dog, which continues to run.)	☒ Close button in the upper-right corner of the Guard Dog window.

□ **NOTE:** If your dial-up Internet account is not set up to dial automatically, connect to the Internet before you use any of the Web-based Help commands.

Opening and closing the Guard Dog Home screen

After you install Guard Dog, the Home screen opens automatically the first time. You can open it yourself in several different ways.

To open the Guard Dog Home screen

- Do one of the following:
  - Click Start in the Windows taskbar, point to Programs, point to Guard Dog, then click Guard Dog.
  - Double-click the Guard Dog shortcut icon on the Windows desktop.
  - Right-click the Guard Dog icon in the Windows taskbar, then click Run Guard Dog.

To close the Guard Dog Home screen

- Click the ☒ button in the upper-right corner of the Guard Dog Home screen.
  Part of Guard Dog remains active to monitor your PC for potential danger. For more information, see “What Guard Dog does while your PC is running” on page 21.

Performing a CheckUp

After completing the interview, you'll want to find out how your PC may be at risk. CheckUp examines your PC for privacy, security, and virus problems and then guides you through fixing any problem it finds. If you are using the settings suggested by Guard Dog in the interview, you need only run CheckUp right after you install Guard Dog and then every month or so. If you reduce the level of protection, you should run CheckUp more frequently.

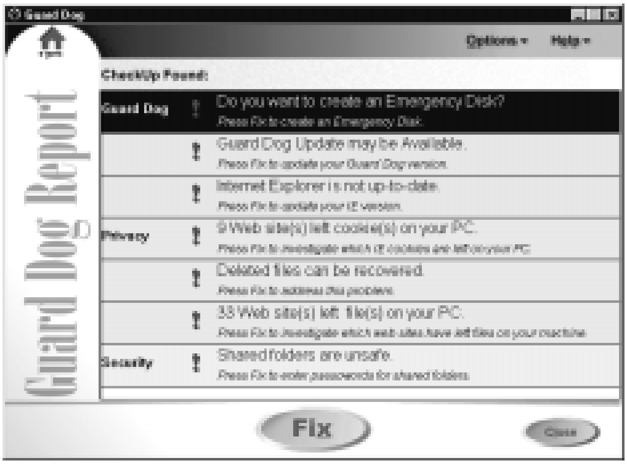
You can also change what checks the CheckUp performs. For example, if you already had virus protection before installing Guard Dog, you may want to turn off Guard Dog's Virus Check. For more information, see "Changing CheckUp Settings" on page 32.

To perform a CheckUp

1. Click CheckUp on the Guard Dog Home screen.

   When the CheckUp finishes, Guard Dog displays a report describing any problems it discovered. (Figure 3-3 on page 19)

Figure 3-3. The Guard Dog Report screen



CheckUp Found:

Guard Dog	!	Do you want to create an Emergency Disk? Press Fix to create an Emergency Disk.
	!	Guard Dog Update may be Available. Press Fix to update your Guard Dog version.
	!	Internet Explorer is not up-to-date. Press Fix to update your IE version.
Privacy	!	9 Web site(s) left cookie(s) on your PC. Press Fix to investigate which IE cookies are left on your PC.
	!	Deleted files can be recovered. Press Fix to address this problem.
	!	33 Web site(s) left file(s) on your PC. Press Fix to investigate which web sites have left files on your machine.
Security	!	Shared folders are unsafe. Press Fix to enter passwords for shared folders.

2. To view a problem that Guard Dog has identified, highlight the item and click Fix.

3. Read the Guard Dog recommendation and then click the appropriate button. If you want more information, click Help, then click Help for this screen.

   A check mark appears next to each problem that you fix.

4. Repeat steps 2 and 3 for each problem that you want to fix.
5. When you have finished selecting all the fixes you want, click Close.

Updating Guard Dog

Guard Dog can keep up with new viruses and Internet threats when you update its program files and virus patterns over the Internet. Using McAfee Software Oil Change technology, you select the updates you want and they are downloaded to your PC and installed automatically.

Guard Dog is set up to remind you monthly to retrieve updates.

NOTE: If you purchased Guard Dog on CD, you should run Update even if you've just installed Guard Dog. In the time between when the CD was created and when you installed it, new virus patterns are likely to be available.

To update the Guard Dog program or virus pattern files

1. If you normally connect to the Internet before you start your browser, start your Internet connection now.
2. On the Guard Dog Home screen, click Update.
   Oil Change will start and begin looking for updates to Guard Dog. If an update is available, it is displayed in the Supported Applications and Drivers dialog box.
3. Select the update. The update description appears in the box below the list.
4. Click Install to download the update.
5. When the Install dialog box appears, click Auto Install.
6. Follow any instructions that appear on your screen. Click Finish to complete the AutoInstall.
7. After you have retrieved all the updates you want, click Close.

Viewing the Log

On the Guard Dog Home screen, click Log to view a list of all the interactions you've had with Guard Dog, including the date and time of the action. You can:

- Print a copy of the Log.

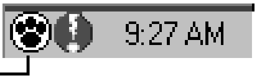
- Save the Log as a text file.
- Clear the entries in the Log.

NOTE: For step-by-step directions on working with the Log, see Guard Dog Help.

What Guard Dog does while your PC is running

While you use your PC, Guard Dog is on the lookout for potential privacy, security, and virus problems and takes action when it finds a problem. (Guard Dog uses the information stored in Protection Settings to determine what to monitor and how to react.) You can tell when Guard Dog is working because its icon appears in the Windows taskbar as shown in Figure 3-4.

Figure 3-4. The Guard Dog icon in the taskbar.



Right-click to display the Guard Dog shortcut menu

NOTE: If you see a Guard Dog alert message, see “Responding to Guard Dog alert messages”later in this chapter.

Using the Guard Dog shortcut menu

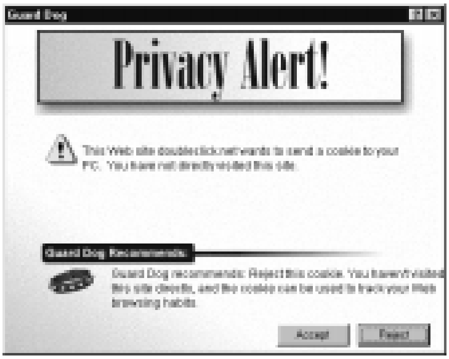
Even when you aren’t running the main Guard Dog program, you still have quick access to several features using the shortcut menu. Right-click the Guard Dog icon on the Windows taskbar to display this menu. From the shortcut menu you can:

- Start the Guard Dog main program.
- Display Browser Buddy, which lets you retrieve your Internet passwords and displays statistics on how many cookies have been allowed or blocked, and how often it has cleared search information.
- Display Protection Settings, which lets you change how Guard Dog is set up.
- Display Windows help for Guard Dog.
- Encrypt and decrypt files that are protected by File Guardian.
- Close the part of Guard Dog that monitors your PC while Windows runs.

Responding to Guard Dog alert messages

Guard Dog works as you work to guard your privacy and security. When Guard Dog detects a potential problem, it either handles the problem automatically or warns you with an alert message (Figure 3-5) based on your Guard Dog settings.

Figure 3-5. Guard Dog alert messages warn you of potential problems



This Web site doubleclick.net wants to send a cookie to your PC. You have not directly visited this site.

Guard Dog recommends: Reject this cookie. You haven't visited this site directly, and the cookie can be used to track your Web browsing habits.

Each alert message tells you what potential problem triggered the message and Guard Dog’s recommendation on how to respond. If you want more information about the problem, click the Question Mark button (Figure 3-6) and then click anywhere inside the alert message.

Figure 3-6. The Question Mark button displays help information

If you find over time that you are being alerted to potential security risks too often, you can adjust the alert message settings in Protection Settings. Cookie Blocker and Gatekeeper require a period of adjustment before Guard Dog has learned to address your concerns with the least amount of disruption.

For information on specific alert messages, see Chapters 4, 5, and 6.

TIP: If you decide you no longer want to see an alert message, use the question mark (?) button in the alert message to find out what setting to change. All of the settings that control the alert messages are located under Protection Settings in the Options menu.

Using Browser Buddy to retrieve or store your Web site passwords

You can depend on Guard Dog to help you as you navigate the intricacies of the Web. When you connect to Web sites that require a name and password, you can use Browser Buddy to:

- Drag your username or password from Password Manager and drop it on the login form for the Web site.
- Add new password information for a Web site.

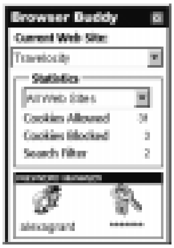
Browser Buddy can also tell you how many cookies have been allowed or rejected by Cookie Blocker and how many times search information has been blocked by Search Filter.

TIP: Browser Buddy always remains displayed on top of any programs open on your screen. If Browser Buddy is located in an awkward position, you can close it and reopen it as needed.

To open Browser Buddy

1. Right-click the Guard Dog icon on the Windows taskbar, then click Browser Buddy.

Figure 3-7. Browser Buddy



To add a new username and password

1. In Browser Buddy, select Add New Entry from the Current Web Site drop-down list.
2. In the Web Site box, type the name of the Web site as you want it to appear in the Password Manager list.

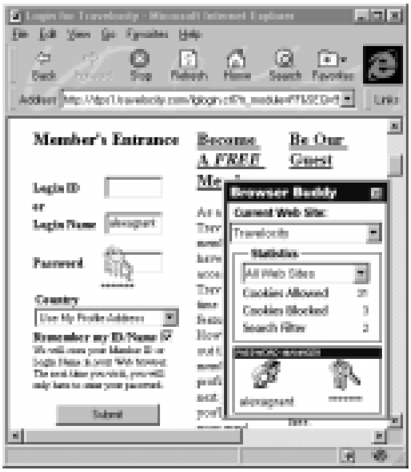
3. In the Username box, type the name by which you identify yourself to the Web site. On the Web site, this may correspond to User Name, Member ID, Member Name, Login ID, or Login Name, and so on.
4. In the Password box, type the password that confirms your identity. (In Password Manager, Guard Dog displays one asterisk for each character in your password.)
5. Click OK.

To retrieve your username and password

1. In Browser Buddy, select the site name if it doesn't appear automatically in the Current Web Site list.
2. Drag your username or password from the Password Manager box to appropriate field in your Web site's login form. (Figure 3-8)

   The text appears in the field. (If the site that you are logging into displays your password text as a series of asterisks (*), Guard Dog will display one asterisk for each character in your password.)

Figure 3-8.



3. Continue logging in as usual to the Web site.

Using file encryption

File encryption translates a file into a “secret” code that makes the file unreadable. You must decode or *decrypt* the file before you can use it. The file encryption in Guard Dog is designed so that you can easily encrypt or decrypt all of the files that you designate for encryption in File Guardian.

□ **NOTE:** Before you can encrypt a file, you must add it to the Guarded Files list in File Guardian. For step-by-step instructions on adding a file to the Guarded Files list, see Guard Dog Help.

To encrypt or decrypt files

- Right-click the Guard Dog icon on the Windows taskbar, then click Encrypt File Guardian files or Decrypt File Guardian files.

Customizing Guard Dog™ 4

Restarting the Interview

Using the Interview is the easiest way to change the settings for Guard Dog. If you want direct control over the settings, see “Changing Protection Settings”in the next section.

To start the Interview

1. In the Guard Dog Home screen, click Options, then click Interview.
2. Follow the instructions on your screen. For more information, see “Using the Guard Dog interview” on page 13 or refer to Guard Dog Help.

Changing Protection Settings

With Guard Dog, you decide how much security and privacy you want or need, how much of a risk you are willing to take with your personal data, and how often you want to be alerted to a potential problem and asked to decide what to do.

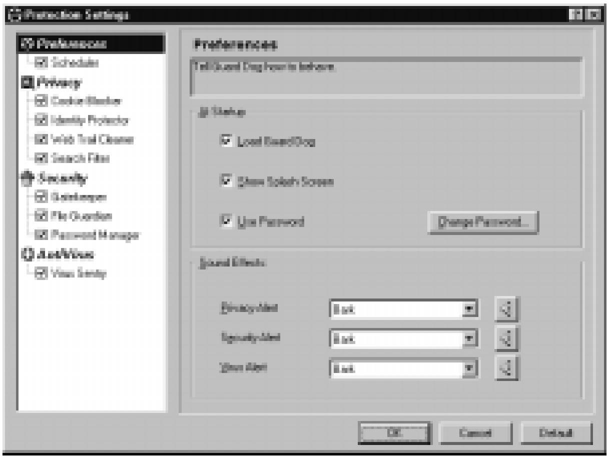
If you find that you are being alerted too often to potential security risks, you can adjust Guard Dog’s security settings. Features like Cookie Blocker and Gatekeeper require a period of adjustment before your security concerns are addressed with the fewest interruptions.

To specify Guard Dog options:

1. Click Options on the Guard Dog Home screen. Then click Protection Settings.
2. To turn on or off any feature, select or clear the check in the check box next to the feature name, as shown in Figure 4-1 on page 28.

When you turn off a feature, you turn off all Guard Dog monitoring for that feature.

Figure 4-1. Protection Settings dialog box



Protection Settings

- Preferences
  - ☑ Scheduler
- Privacy
  - ☑ Cookie Blocker
  - ☑ Identity Protector
  - ☑ Web Trail Cleaner
  - ☑ Search Filter
- Security
  - ☑ Gatekeeper
  - ☑ File Guardian
  - ☑ Password Manager
- AntiVirus
  - ☑ Virus Sentry

Preferences

Tell Guard Dog how to behave.

At Startup

☑ Load Guard Dog

☑ Show Splash Screen

☑ Use Password

Sound Effects

Privacy Alert: Bark

Security Alert: Bark

Virus Alert: Bark

3. To change individual settings for a feature, first make sure that the feature is turned on.

   - Select the feature in the list so that its option settings appear in the pane on the right.
   - Adjust settings for the feature as appropriate.
     To find out what a setting does, click the question mark (?) button in the upper-right corner of the dialog box, then click on the setting.

     Preferences settings are described in the next section of this chapter. Privacy settings are described in Chapter 4, Security settings are described in Chapter 5, and AntiVirus settings are described in Chapter 6.

Preferences settings

The Preferences settings affect all of Guard Dog.

Table 4-1.

Use	To
Load Guard Dog	Start Guard Dog monitoring your PC for potential problems when Windows starts.
Show Splash Screen	Briefly display the Guard Dog logo when Windows starts.
Use Password	Protect your settings from unauthorized changes. Click the Change Password button to change an existing password.
Sound Effects	Set the sound Guard Dog plays when it displays a Privacy, Security, or Virus Alert message. Click the Speaker button to preview the selected sound.

Scheduling Guard Dog actions

Guard Dog comes with a number of items that you can schedule. You can schedule Guard Dog to perform time-consuming tasks, such as a virus check on all files, while you are away from your computer. Remember to leave your PC on during the scheduled time period.

To schedule an event

1. Click Options on the Guard Dog Home screen. Then click Protection Settings.
2. In the pane on left side of the screen, make sure that a checkmark appears in the check box next to Scheduler. If necessary, click the check box to select it.
3. Click the word, Scheduler.
4. Click Add.

5. Select an event to schedule. See Table 4-1 on page 30 for a description of the types of items you can schedule.

6. The Add Schedule Wizard guides you through selecting an interval, date, and time for the event.

7. Click Finish to add the event to your Scheduler list.

Table 4-1. List of events that can be scheduled

Use	To
Schedule a Virus Check on all files	Check for viruses in all files on all local drives, including floppy drives, CD-ROM, and removeable media drives.
Schedule a Virus Check on high-risk files	Check for viruses in program and document files on all local drives, including floppy drives, CD-ROM, and removeable media. This event is automatically scheduled to occur when Windows starts.
Schedule a Virus Check on changed files	Perform a Virus Check only on files that have been created or modified after the date and time of the last check. (It will check all files if a Virus Check has never been performed.)
Schedule encryption of my File Guardian files	Encode files that are in the Guarded Files list of File Guardian.
Schedule decryption of my File Guardian files	Decode encrypted file that are in the Guarded Files list of File Guardian.
Schedule removal of the deleted files on my PC	Write over data that remains after files are permanently deleted from your Recycle Bin. (The data from a file that has been deleted from your Recycle Bin, remain on your hard disk until overwritten. A sophisticated disk editor could be used to retrieve the data and recreate the file.)

Table 4-1. List of events that can be scheduled

Use	To
Remind to create an Emergency Disk	Display a reminder message. When you install Guard Dog, this event will be scheduled to occur every four months.
Remind to check for Guard Dog updates	Display a reminder message. When you install Guard Dog, this event will be scheduled to occur every month.

To edit an event in the Scheduler list

1. Select the event in the Scheduler list.
2. Click Edit. The Add Schedule Wizard guides you through the selections.

To remove an event in the Scheduler list

1. Select the event in the Scheduler list.
   - To select contiguous events, click the first event, then hold down the Shift key and click the last event.
   - To select non-contiguous events, click the first event, then hold down the Ctrl key and click each desired event.
2. Click Remove.

Changing CheckUp Settings

Guard Dog can run a complete or partial CheckUp based on the selections you make in CheckUp settings.

Table 4-2. CheckUp Settings

Category	Name of Check	Description
Guard Dog	Emergency Disk	Reminds you that you don't have an Emergency Disk or that the disk you made may need updating.
	Guard Dog Updates	Reminds you that Guard Dog may need updating.
	Browser Version	Warns you if you are not using the most recent version of Microsoft® Internet Explorer and Netscape Navigator™ browsers and offers to update your browser software. (Older browser versions have more security risks.)
Privacy Checks	Identity Protection	Looks for files containing personal information and lets you protect them.
	Cookie	Lists the cookies being stored on your PC and lets you remove them.
	Search Filter	Looks to see if information exists from the last search in your Web browser and allows you to remove that information.
	Web Trail	Lets you removes evidence of your Web browsing—cached browser files, all URLs referenced in your browser's preferences and history lists, and ActiveX controls—from your PC's hard drive.
Security Checks	Gatekeeper	Reports the names of the programs that you have approved for Internet access over your dial-up or network connection and lets you change your mind about allowing automatic Internet access.
	File Guardian	Searches for sensitive files (such as e-mail messages or financial files) that contain information that you want to keep private and lets you protect them.

Table 4-2. CheckUp Settings (Continued)

Category	Name of Check	Description
	Password	Looks to see if you have any shared files/folders on your PC and guides you through password protecting them.
Virus Check	Virus Check	Looks on all selected drives or folders for virus-infected files that match the selection setting for What to scan at CheckUp in Virus Sentry. For more information, see “Why should I change my Virus Sentry settings?” on page 54.

To turn on or off specific checks

1. In the Guard Dog Home screen, click Options, then click CheckUp Settings.
2. Select or clear specific check box next to each option.
3. In Virus Check, select the drives or folders that you want to scan for viruses.
4. Do one of the following:
    - To save these settings and return to the Home screen, click Apply.
    - To abandon these changes and return to the Home screen, click Cancel.

Privacy Features 5

Guard Dog's Privacy features protect browsing and personal information that you don't want to go out on the Internet.

What Cookie Blocker does

Cookies are small files that your Web browser stores on your PC at the request of a Web server. Each time you view a Web page from the Web server, your browser sends the cookie back to the server. These cookies can act like a tag, which lets the Web server track what pages you view and how often you return to them. Some Web sites, such as Microsoft Expedia™, use cookies to store your password and preferences so that you can automatically log on to the site. For a more detailed description of cookies, see "What are cookies and how are they used?" on page 69.

Guard Dog's Cookie Blocker offers three options for controlling the use of cookies on your PC. Guard Dog can:

- Reject all cookies.
- Accept all cookies.
- Display an alert message each time a cookie is sent to your browser. The alert displays the name of the entity trying to set the cookie, and advises you whether or not to accept the cookie.

  When setting up Cookie Blocker in Protection Settings, you can select one option for *direct sites* and another for *indirect sites.* Direct sites are those that you deliberately connect to by typing the URL; clicking a link in a Web page; or by selecting from your list of bookmarks or favorite sites. Indirect sites are those that you access because the site you are connecting to directly displays content from another site as part of its own content. For example, if you went directly to Cool_site.com, it could display an ad from Ads-r-us.com (the indirect site) in a separate frame in the Cool_site page.

  If during the Interview, you accepted Guard Dog's recommendation on how to respond to cookies, Cookie blocker will:

- Automatically allow cookies to be accepted from direct sites.
- Display an alert message when an indirect sites tries to set a cookie.

Responding to a Cookie Blocker alert message

If during the Interview, you told Guard Dog to prompt you for action then it will display the Cookie Blocker alert message the first time a site tries to set a cookie.

You can respond to the alert message in the following ways:

Table 5-1.

If you choose	Guard Dog does this
Accept always	Accepts the cookie and adds the site to the Allowed list. The next time you go to that site, all cookies from that site are allowed automatically.
Never accept	Rejects the cookie and adds the site to the Rejected list. The next time you go to that site, all cookies from that site are refused automatically.(In some cases, the cookie may be written to your local hard disk, but your privacy is protected because the cookie is nevr sent back to the requesting page.)

Each time that you visit a site that appears in either the Allowed or Rejected list, Guard Dog adds the number of cookies accepted or rejected to the list. You can see the totals for a Web site in Browser Buddy.

If you change your mind about a site, you can remove it from the Allowed or Rejected list in Cookie Blocker settings. The next time that you visit that site it will be as if you are visiting it for the first time. If you want to remove cookies for a site from which you’ve previously accepted cookies, run a CheckUp and remove the cookies for that site.

TIP: You can run CheckUp so that it only looks for cookies. On the Guard Dog Home screen, click Options, click CheckUp Settings, then clear all options except Cookie Check. After you are finished with the CheckUp, don’t forget to change back your settings.

Why should I change my Cookie Blocker settings?

If you want a good level of privacy protection without having to see any Cookie Blocker alert messages, use the recommended settings—always accept cookies from sites that you visit directly and decide on a case-by-case basis whether to accept cookies coming from sites that you haven't visited directly. You may want to change your settings under the following circumstances:

Table 5-2.

If you	Use this option
Want the least number of cookies set and highest assurance of privacy.	Reject for both Direct Sites and Indirect Sites. If a site requires you to accept a cookie, you can change this setting temporarily to Prompt.
Always want to know when cookies are sent.	Prompt for both Direct Sites and Indirect Sites. Be prepared to respond to a large number of alert messages. After you respond to the Cookie Blocker alert message, you won't see additional alert messages for that site.
Are not concerned at all about cookies.	Either turn off Cookie Blocker or change the Indirect Sites setting to Accept. You should choose the second method if you want to keep a total of the cookies added to your PC, which you can view in Browser Buddy.

What Identity Protector does

It is easy to forget that when you send information over the Internet, it doesn't go directly from your computer to the computer that is storing the Web page information. Instead, the information can pass through many computers before it reaches its final destination.

Identity Protector can keep your software from sending any personal information that you specify out over the Internet to an unsecure site. Although you don't have to worry about a site when it using a secure connection, there are many Web sites that use a secure connection only when dealing with credit card transactions. (For more information, see "Privacy on the Web" on page 62.)

If more than one person is using your computer, make sure that you create a Guard Dog password. If the person using your computer doesn't enter the Guard Dog password, Guard Dog automatically replaces any protected personal information sent to an unsecure site with the text, “xxxx.” For example, if your child tries to order the latest CD without entering your Guard Dog password, Guard Dog replaces your credit card number with “xxxx xxxx xxxx xxxx.”

Identity Protector offers three responses to when an application tries to send out information over the Internet to an unsecure site:

- Let the information go out.
- Block the information from going out.
- Display an alert message when any application tries to send the information over the Internet to an unsecure site. This is the response Guard Dog sets up when you add information to protect in the Guard Dog Interview.

Responding to an Identity Protector alert message

During the Interview, Guard Dog asked you to enter your personal and financial information that you want to protect. Guard Dog displays the Identity Protector alert message the first time an application tries to send out this information to an unsecure site.

You can respond to the alert message in the following ways:

Table 5-3.

If you choose	Guard Dog does this
This time only	Let the information go out just this time.
Not this time	Prevents the information from going out this time.

Why should I change my Identity Protector settings?

You may want to change your settings under the following circumstances:

Table 5-4.

If you	Use this option
Are the only person using your PC and you don't want to be alerted every time.	Enter all of the information that you want to prevent from going out and select Allow Always. Create a Guard Dog password. If the Guard Dog password is not entered after you start Windows, an unauthorized user of your PC can't view or send out your personal information.
Have more than one person using your PC.	Enter all of the information that you may want to prevent from going out and select Allow Always or Ask Before Blocking. For information that you always want to prevent from going out, select Block Always. Create a Guard Dog password. If the Guard Dog password is not entered after you start Windows, any information entered in Identity Protector will be blocked from being sent out.
You want to be warned any time this information is being sent out.	Enter all of the information that you may want to prevent from going out and select Ask Before Blocking.

NOTE: When Guard Dog asks for your password and you enter it, the password stays in effect until you restart Windows. If you've entered your password and want to block others from sending out your personal information, restart Windows before letting anyone else use your PC.

What Web Trail Cleaner does

As you surf the Internet, your browser stores information that makes your browsing experience more satisfying. It uses the information as follows:

Table 5-5.

Your browser uses	To
Cached files	Speed up the display of Web page elements such as graphics.

Table 5-5.

Your browser uses	To
URLs visited	Display a list sites that you’ve visited using Web addresses.
History	Display a list sites that you’ve visited using Web site names.

The files left on your PC can be viewed by others and depending on your browser’s settings, can take up many megabytes of disk space.

If you accepted Guard Dog’s recommendation during the interview, Guard Dog displays the Web Trail Cleaner alert message when you close your browser.

Responding to the Web Trail Cleaner alert message

You can respond to the alert message in the following ways.

Table 5-6.

If you choose	Guard Dog does this
Clean	Deletes all of the cached files, history and URL information associated with the selected Web site (Domain). Select a site for cleaning by selecting the check box next to the site name. To sort by a column heading, click the heading name.
Don’t clean	Closes the Alert message and continues closing your browser.

By default Guard Dog selects the sites that are not bookmarked (that is, part of your list of favorite sites) because it is less likely that you’ll return to these sites. If you don’t return to a site, the cached files for the site are never used again—they just sit and take up disk space until they are ultimately deleted by your browser.

If you later want to delete the files that you’ve left behind, run the Guard Dog CheckUp.

Why should I change my Web Trail Cleaner settings?

You may want to change your settings under the following circumstances:

Table 5-7.

If you	Use this option
Want to see exactly what files are being deleted.	Prompt to Clean Up after closing Web browser.
Want to remove all traces of your browsing.	Automatically Clean Up after closing Web browser. (Clear the check box for “Keep bookmarked items.”)
Want to remove files only for Web sites that you haven’t bookmarked or added to your list of favorites.	Automatically Clean Up after closing Web browser. Keep bookmarked items.

What Search Filter does

When you perform a search in your Web browser, the search information is displayed in the address box of your Web browser. When you go to another site, the search information is retained by your browser and can be extracted by the next site you visit. Search Filter blocks this information from being passed along to the next site.

If you have Search Filter selected in Security Settings, Guard Dog automatically removes search information before you go to another Web site. Guard Dog does not display an alert message for this feature, but you can see the number of times Search Filter blocks this information in Browser Buddy.

Security Features 6

Guard Dog's security features safeguard your Internet connection and protect the files on your PC from prying eyes and destructive programs.

What Gatekeeper does

Gatekeeper lets you control what programs have access to your Internet connection. Gatekeeper also can warn you about any of these potentially harmful actions:

- Your browser is directed to a harmful site—one that has been known to contain virus-infected files, Trojan horses, prank or destructive ActiveX controls, or other security concerns.
- A program silently uses your modem to connect to another computer.
- A program starts up another program.
- A program sends out over the Internet a number that follows a common credit card number pattern.

Responding to a Gatekeeper alert messages

Guard Dog can display five different Gatekeeper-related alert messages. If you are using the default settings suggested by the Interview, you will see the messages related to Internet access, harmful sites, programs starting another program, and programs sending out credit card-like numbers.

Internet access alert message

Each time you start a program that attempts to use your Internet connection, Guard Dog checks to see if that program is in the list of programs allowed to access the Internet. If the program is not in the list, Guard Dog displays an alert message to tell you that the program is trying to connect to the Internet and asks you how to deal with the program.

Because Guard Dog displays an alert the first time you start an Internet program, you may want to start each of the Internet-connected programs you use regularly in order to get those alerts out of the way at one time.

You can respond to the Internet access alert message in the following ways:

Table 6-1.

If you choose	Guard Dog does this
This time only	Allows the program to access the Internet this time only and warns you the next time it tries to access the Internet.
Allow always	Allows the program to access the Internet at any time. In Protection Settings for Gatekeeper, the program is added to the list of programs allowed to automatically access the Internet. If you decide later that you do not want this program to use your Internet connection, select its name and click Remove.
Not this time	Prevents the program from accessing the Internet. This choice stays in effect until the next time you restart Windows or for Internet Explorer 4 users, until you close your browser. Use this option if you want Guard Dog to warn you the next time the program tries to access the Internet.

Harmful site alert message

Before you can connect to harmful site, Guard Dog will display an alert message, “Your browser is visiting *Sitename*, a Web site that may harm your PC or data.”

You must immediately close your browser to end your browser’s connection to this site. The faster you close your browser, the less time the site has to transfer harmful data to your PC.

If you want to view the Web site anyway, click Continue.

Program starts up another program message

When another program starts to run another program, Guard Dog checks to see if you’ve authorized this action. If you haven’t allowed the program to always open the other program, Guard Dog displays an alert message.

You can respond to the alert message in the following ways:

Table 6-2.

If you choose	Guard Dog does this
Allow always	Lets the program start the other program.
Not this time	Prevents the program from starting the other program just this time.
This time only	Lets the program start the other program just this time.

Any credit card number goes out message

When a program sends a number resembling a credit card number over the Internet, Guard Dog displays an alert message.

You can respond to the alert message in the following ways:

Table 6-3.

If you choose	Guard Dog does this
Not this time	Prevents the program from sending the number this time.
This time only	Lets the program send the number just this time.

Why should I change my Gatekeeper settings?

The Gatekeeper settings suggested by the Interview will display the fewest number of alert messages. If you are using an older browser version or just want a higher level of security, you may want to change your settings under the following circumstances:

Table 6-4.

If you	Use this option
Want to be warned when the site that you are going to has been known to cause damage, e.g. contains virus-infected files, Trojan horse, prank or destructive ActiveX controls, or other security concerns. (To keep Guard Dog’s list of harmful sites current and effective, use Update monthly.)	Going to harmful sites.
Want to be warned when a program is using your modem to dial out.	My modem dials silently.

Table 6-4.

If you	Use this option
Want to be warned when a program starts up another program. Many newer programs will warn you before doing this, but older programs may not do so. For example, Internet Explorer 4 uses “helper programs” to display documents.	Program tries to launch another program.
Want to be warned before any number that resembles a credit card number is sent out over the Internet. To protect specific numbers, see “What Identity Protector does” on page 37.	Any credit card number goes out.
Want to see what programs you have allowed automatic access to the Internet. (A program is added to the list when you click Accept Always in the Internet access alert message.) If you change your mind, you can remove an program from the list. You will be warned the next time that program tries to access the Internet.	These programs are always allowed access to the Internet

What File Guardian does

File Guardian can protect files that contain your sensitive data from being opened, renamed, copied, moved, or deleted. For added protection, you can even encrypt files protected by File Guardian. Guard Dog can also alert you if an program attempts one of the following potentially harmful activities:

- A program attempts to reformat your hard drive.
- An ActiveX control attempts to delete files on your hard drive.
- An ActiveX control attempts to scan files on your hard drive.
- A program attempts to access your system password files.

When Guard Dog displays an alert message, you can decide if the program should be allowed to continue the operation or not.

Responding to a File Guardian alert messages

Guard Dog can display five different File Guardian-related alert messages. If you are using the default setting suggested by the Interview, you will see only the guarded file, ActiveX scan, ActiveX delete, and drive format messages.

Guarded file alert message

You tell File Guardian which files to guard on your hard drive and what programs can be used to open the files. If an unauthorized application attempts to access a guarded file, Guard Dog displays an alert message that tells you what application is trying to open which file.

You can then decide whether you want to give the program in question access to the file. If you did not run the unauthorized program yourself, you should immediately investigate the program to determine its source.

Table 6-5.

If you choose	Guard Dog does this
Allow always	Permits the program to open the file and adds the program to the list of programs that are authorized to access the file without further warnings.
Not this time	Stops the program from opening the file and warns you the next time the program tries to open the file.

ActiveX scan alert message

There are legitimate reasons for allowing an ActiveX control to read through, or *scan*, all of your files. For example, you can go to one site on the Web that uses an ActiveX control to look for viruses on your PC. However, if a site begins to scan your files without warning you, Guard Dog gives you a chance to think about how much you trust the site.

When Guard Dog detects an ActiveX control scanning the files on your PC, it displays an alert message that tells you what ActiveX controls is scanning your hard drive.

You can respond to the alert message in the following ways:

Table 6-6.

If you choose	Guard Dog does this
Not this time	Stops the ActiveX control from running this time. If you change your mind, reload the page in your browser and click **This time only** the next time Guard Dog displays its ActiveX scan message.
This time only	Permits the ActiveX control to scan your drive just this time.

ActiveX delete alert message

There are legitimate reasons for allowing an ActiveX control to delete files. For example, if a control installs special software on your PC to let you interact with its Web site, the control may need to delete files that it created for temporary use. However, if a site doesn't warn you and begins to delete files, Guard Dog gives you a chance to see what file is being deleted and think about how much you trust the site.

When Guard Dog detects an ActiveX control deleting files on your PC, it displays an alert message that tells you the name of the control.

You can respond to the alert message in the following ways:

Table 6-7.

If you choose	Guard Dog does this
Not this time	Stops the ActiveX control from running this time. If you change your mind, reload the page in your browser and click **Allow this time** the next time Guard Dog displays its ActiveX delete message.
This time only	Permits the ActiveX control to delete files just this time.

Drive format alert message

When a format command is started, Guard Dog doesn't know whether you told your PC to format a Zip disk or whether a rogue ActiveX control has started to format your hard disk. You know that this activity is legitimate when you start the formatting command or if you know that a program you are using needs to format a hard disk (or a Zip or Jaz disk).

When Guard Dog detects a format command, it displays an alert message that tells you which program started the format command.

If you don’t know why your disk is being formatted, note the name of the program in the alert message and then turn off your computer using its power switch. If the program has the letters OCX as part of its name, it is an ActiveX control. Do not restart your browser until you have run a Guard Dog CheckUp and removed the suspicious ActiveX control from your PC.

Click **Continue** if you want the program to format your disk.

Why should I change my File Guardian settings?

You may want to change your settings under the following circumstances:

Table 6-8.

If you	Use this option
Want to be warned when an ActiveX control looks through the files on your PC. This may happen legitimately if the control needs to find a file to use. If you are concerned, check with the site that sent you the control.	ActiveX scans my drive
Want to be warned when an ActiveX control deletes a files. This may happen legitimately if the control is deleting older or temporary files that it uses. If you are concerned, check with the site that sent you the control.	ActiveX deletes files from my drive
Want to be warned when any program tries to format any of your drives. An alert message appears whenever you format a floppy disk, other removable media, or hard disk. You may want to turn this option off temporarily if you are going to format a lot of disks and don’t want to see any messages.	My drive is being formatted

Table 6-8.

If you	Use this option
Want to be warned when any program accesses your Windows password files (any file with the .pwl extension located in the Windows directory). Windows functions that are password-protected use these password files.	Password files are accessed
Want to prevent any program from opening a file or files. For further protection, you can have Guard Dog include the file when you encrypt files. You can protect individual files, files in a specific folder, files of the same type, files on the same drive.	Guarded files

NOTE: For step-by-step instructions on adding, editing, or removing files in the Guarded Files list, allowing a program to access a guarded file, or encrypting or decrypting files, see Guard Dog Help.

What Password Manager does

Password Manager lets you store your various Web site login names and passwords in one secure location. When you are visiting a Web site that requires this information, you can drag it from Browser Buddy to the form displayed in your browser.

In Protection Settings, you can:

- View your list of stored login names and passwords.
- Add a record.
- Edit a record.
- Remove a record.

You can also add a record in Browser Buddy. For more information, see “Using Browser Buddy to retrieve or store your Web site passwords” on page 23.

To add a password record

1. In the Guard Dog Home screen, click Options, then click Protection Settings.
2. Click Password Manager. (If the check box next to Password Manager is not selected, you won't be able to add, edit, or remove records.)
3. Click Add.
4. Type the information that you want to store in the record.
5. Click OK.

To edit a password record

1. In the Password Manager list, do one of the following:
   - Double-click the record you want to edit.
   - Click the record you want to edit, then click **Edit**.
2. Change the information that you want to store in the record.
3. Click OK.

To remove a password record

- In the Password Manager list, click a record to select it, then click Remove.

Using AntiVirus Features 7

Guard Dog's AntiVirus features can fix most existing virus problems and prevent them from recurring. For general information on viruses, see Appendix B.

Looking for viruses with CheckUp

Guard Dog comes set up to perform a virus check as part of CheckUp. It uses the settings in CheckUp Settings to determine which drives and folders to check (by default, your local drives—hard disks, floppy disks, and other removable media). It uses the settings in What to check in Virus Sentry to determine what types of files to check (by default, all program and document files). If a virus-infected file is found, it appears in the CheckUp Found list.

Viruses are different from other problems found by Guard Dog in that you can either clean (remove the virus from the file) or delete the file. If Guard Dog tries to clean a file but the virus has irreparably damaged the file, you can only delete the file to get rid of the virus.

Continuing virus protection

If you accepted the recommended virus protection in the Interview, Guard Dog is set up to protect you:

- When you start your PC, Guard Dog checks your DOS startup process for viruses in memory and boot sector or partition table viruses on your hard drive—the boot sector and partition table contain critical startup and system information.

- Every time you start Windows, Guard Dog runs a scheduled virus check that scans all the program and document files on your local disks (hard disks, floppy disks, and other removable media) for viruses.

- When a scheduled virus check runs, it opens Guard Dog and displays the CheckUp progress screen. The CheckUp Report screen displays the virus check results.

- While you are working, Guard Dog checks for viruses whenever you start a program, move or rename files, or read a file from a floppy disk.

- Each month, Guard Dog runs a scheduled virus check that scans all files on your local disks. This check will catch viruses in files that don’t use standard program or document names. To find out how to schedule additional virus checks, see “Scheduling Guard Dog actions” on page 29.

What Virus Sentry does

Virus Sentry lets you set up AntiVirus protection so that it best protects the data on your PC.

Virus Sentry controls:

- When to check for viruses while you are using your computer to:
  - Start a program from the Start menu, a Windows shortcut, or by double-clicking the program in Windows Explorer. This includes programs sent as e-mail attachments.
  - Open a document. This includes documents sent as e-mail attachments.
  - Move or rename files.
  - Read a file from a floppy disk.
- What files to scan while performing a virus check using CheckUp or Scheduler.
- How Guard Dog responds when it finds a virus.
- What files can be skipped while performing a CheckUp or Scheduler virus check.

When Guard Dog finds a virus, it displays an alert message.

Responding to a Virus Sentry alert message

When Guard Dog finds a virus, it displays an alert message.

You should always click Clean. If you click Ignore, Guard Dog will do nothing to the file. If you choose to ignore the alert message, do not open the infected file or you will spread the virus.

Why should I change my Virus Sentry settings?

By default, Guard Dog is set up to provide the best protection, in the fastest manner. You can increase your protection level, but it will take longer to perform a scan.

You may want to change your settings under the following circumstances:

Table 7-1.

If you want to	Use this option
Check for virus infection before a program starts up.	Program execution.
Check an e-mail attachment before it is opened.	E-mail file access.
Check a file before it is opened.	File Open.
Check a file when it is moved or renamed.	Move or Rename.
Check a file if it is stored on a floppy disk or removable media.	Floppy drive read
Check for boot sector or partition table viruses before Windows starts. These viruses may be detected when Windows starts, but they can be cleaned only in DOS.	DOS Startup
Change the scope of what files are checked. This setting affects not only file-related checks but also the scheduled virus checks.	What to Check: All Files checks every file. This is the most thorough, but most time consuming check. Use this setting if you use non-standard file extensions for your program or document files. Program Files checks all program files, such as .Exe, .Com, .Dll file types. This will miss macro viruses, which are found in certain document types. Document Files checks all data files recognized on your PC. This will miss program-related viruses. Program and Document Files checks both program and data files. This is the default setting and the second most thorough check. It will miss only virus-infected files that have been renamed using a nonstandard program or document type.

Table 7-1.

If you want to	Use this option
Want to change how Guard Dog reacts when a virus is found and what options are available for dealing with the virus.	If a virus is found: Automatic Clean tries to remove the virus. If unsuccessful, it will prompt you to delete the file. This is the default setting. Automatic Delete deletes the file from your PC. You may want to use this option if your PC runs unattended and you don’t want an alert message to stop the operation of your PC. Deny Access blocks you from doing anything with the file except for deleting it in Windows Explorer or running a CheckUp to try to clean the file. You may want to use this option if your PC runs unattended and you don’t want to risk anyone having access to infected files on your PC, you want to deal with the file manually. Prompt displays an alert message and allows you to choose to Clean or Ignore the file. Shutdown Computer closes Windows. You may want to use this option if your PC runs unattended and you don’t want to risk anyone having access to infected files on your PC.
Reduce the number of files checked by Guard Dog. This setting affects not only file-related checks but also the scheduled virus checks.	Do not check these files and folders. (By default, Guard Dog doesn’t check files that are in your Recycle Bin.)

NOTE: If CheckUp has reported that your PC is virus free, you may want to turn off the **Virus Check** in **CheckUp Settings** to reduce the amount of time that it takes to complete your CheckUp. This does not disable automatic virus checking. As long as you have all automatic virus checking turned on (**What to Check** settings in **Virus Sentry**), you are not likely to get a new virus.

Keeping virus protection up-to-date

The AntiVirus protection in Guard Dog uses a database of known virus-characteristics when it checks your PC for a virus, but new viruses are always being created and old viruses are always being modified.

The McAfee Software virus research team is constantly watching for these new and changed viruses. As new virus information is discovered, it is added to the pattern file. Once a month, a new pattern file is made available through the Internet. You can retrieve it by clicking your Guard Dog Update button. For more information, see “Updating Guard Dog” on page 20.

It is important to keep this file up-to-date on your PC. Guard Dog schedules a reminder to suggest that you check for a new version of the pattern file each month.

Internet Security and Privacy A

Whom do you trust? On the Internet, this question is difficult to answer—you cannot not see people face-to-face, and cannot be certain exactly who you are dealing with. This chapter provides some background information that will help you understand Internet security and privacy threats, and discusses strategies for using Guard Dog to protect yourself and your computer.

Networks and the Internet

A computer network links individual computers together so they can share data and resources. To network, computers need some means of connection—either a modem or a Network Interface Card (NIC—some computers have NICs already built-in). The modem or NIC is responsible for sending and receiving data through the network. Networks are sometimes called *local area networks* (LAN) because they link the computers at a single locale, such as an office or building. In a small office, computers can be linked directly by connecting them together with cable. This very simple network is called a *peer-to-peer* network, because all of the computers are equal to one another. Windows has peer-to-peer networking capabilities built into the operating system. The increased traffic in larger networks requires the services of a special computer, called a *server*. Servers help larger networks operate by figuring out how to route messages to the appropriate recipient.

The Internet is a vast computer network, connecting computers together from around world and allowing them to work together and share information. When you connect to the Internet, your computer becomes a part of a worldwide network of computers.

TCP/IP is the subsystem

The Internet is based on a system called Transmission Control Protocol / Internet Protocol (TCP / IP). TCP lets computers share data by first breaking it down into little segments called packets. In addition to data, each packet contains the address of the machine sending the packet, and the address of the intended recipient. The TCP part of the system is what is responsible for addressing the data and breaking into packets. IP, the second part of the system, is responsible for routing packets from the sending computer to the recipient computer. Special computers called routers read the address on each packet, and figure out how to route them to the appropriate destination.

Why packets?

Why go through all this trouble, breaking data down into packets? The answer lies in the origins of TCP / IP. TCP / IP, like the Internet itself, is a product of the Cold War. Originally developed by the United States Department of Defense, the Internet was designed to ensure secure communications, even with the multiple communications network failures anticipated during nuclear war. TCP / IP solves the problem of network failure by assuming that a certain amount of noise always exists in the network: Noise may be random data errors or more serious system crashes. If you have ever tried to speak in a noisy room, you know the necessity of repeating yourself—and that is exactly what TCP / IP is designed to do. Breaking data down into packets allows the Internet to seek alternate routes if one route is inaccessible. If a packet cannot get through or arrives damaged, the receiving computer simply requests it again until it arrives successfully.

When you send an e-mail message, for example, it is broken into several packets. Depending on how noisy the network is, each packet may need to be routed over a separate route in order to find its way to its destination. Furthermore, network problems may cause some of the packets to be delayed so they arrive out of order. To compensate, TCP examines each packet as it arrives to verify that it's OK. Once all the packets are received, TCP puts them back in their original order. Of course, all of this happens quickly and automatically, so you will never see the process at work.

The Internet and the Web…what is the difference?

Before the Web, the Internet was mostly command-line driven, and character-based: You had to type in the exact Internet address of the place you wanted to go at a command line. In 1989, Tim Berners-Lee of the European Particle Physics Laboratory proposed a new way to share information over the Internet. The essential feature in Berner-Lee’s vision of the Web is that it links documents together. When you click a link on a Web page, you are automatically connected to another Web site. This linking function, combined with the increasing graphics abilities of home computers, transformed the Internet into a graphically rich place, complete with video, sound, and pictures. By linking information together in a graphically-appealing package, the Web made the Internet more attractive to the typical consumer.

The Internet is a network of linked computers that uses TCP / IP as its underlying messaging system. The World Wide Web (WWW, or just “Web” for short) is hosted by the Internet, and is an ever-expanding collection of documents employing a special coding scheme named Hypertext Markup Language (HTML).

NOTE: HTML is a set of commands designed to be interpreted by Web browsers. An HTML document consists of content (prose, graphics, video, etc.) and a series of commands that tell a Web browser how to display the content.

Privacy and security on the Web

Before the advent of the Web, Internet security usually posed a problem only for system administrators trying to keep meddlesome hackers away from their systems. When the Web arrived, the popularity of the Internet skyrocketed. Almost overnight, people began doing all sorts of potentially sensitive activities over the Internet, including banking and stock transactions, sending personal data to Web sites, performing Web searches, and ordering books and clothes. So, while the Web is responsible for making the Internet more accessible, it also opens up new possibilities for data theft, invasions of privacy, and fraud.

Why does Internet privacy matter to me?

Step back and consider the range of sensitive transactions we make every day. As an example, consider a simple ATM transaction: We assume that following conditions prevail whenever we use our ATM cards:

- **Privacy**: Only you and the intended recipient can access the transaction information. The PIN you use to access your bank account provides a fairly high level of privacy—as long as you don’t share your PIN with others, and don’t leave your card lying around, your checking account balance is safe from prying eyes.
- **Integrity**: Nothing can intervene and change the information during the transaction. When we take twenty dollars out of our checking account, we have a reasonable expectation that the ATM will not add an extra zero.
- **Trust**: You can trust that the recipient is who they claim to be; the recipient can trust that you are who you claim to be.

Organizations like banks and insurance companies are legally obliged to abide by federal statutes that govern the sanctity of your transaction information. The problem with Internet is that it has not yet evolved well-established institutional mechanisms that guarantee the sanctity of your information.

Privacy on the Web

Who is snooping?

Hackers are a breed of human being that thrive on gaining illegal access to computers in order to access, steal, and sometimes corrupt data. Many hackers are quite benign: Breaking into a secure system is a challenge and a thrill. But some computer hackers think that if they don't care for someone or some organization, it is OK to break in to their computers and wreak havoc. Others hackers think that the on-line theft of money and resources is legitimate, as long as it goes to support more hacking.

Snooping and sniffing

Since its inception, the Internet has been (and largely remains) an open network. Openness means that information on the Internet travels without any special security: Anyone who can monitor network traffic can intercept it. This sort of monitoring is called "sniffing," and is easy to perform using "sniffers." Sniffers are programs (or hardware devices) designed to monitor data traveling over a network. Originally, sniffers were designed to help network administrators track down networking problems. Unfortunately, the same tool can also be used to steal information. Sniffers are insidious and difficult to detect.

Sniffing often begins when a hacker breaches the security of a local Internet Security Provider (ISP). A hacker does not need physical access to the ISP's premises—sometimes a telephone line is sufficient (although it is also possible to sniff with physical access to network cables). Once a hacker compromises an ISP's system, the network traffic that travels through the ISP is no longer secure.

Web servers and firewalls

Secure transactions are only one part of the problem. When an ISP's Web server receives information, the ISP must be able to keep the information safe. Hackers like to attack the security of Web servers because Web server security is still in its infancy. As a consequence, Web administrators assume that a Web server is open to attack, and try to keep them decoupled from other, mission-critical computers. Some Web applications must, however, interact with corporate databases, an open door to a clever hacker. One form of security technology called a "firewall" can close the door, but firewalls are often maintained poorly, and even in the best environment, cannot safeguard certain services.

What can I do to keep my stuff safe?

With sniffer in place, a hacker can intercept credit card numbers and other private information by capturing data transmissions, and then using pattern-matching algorithms to filter out the valuable information. Intercepted credit card info can be sold to criminals, intent on committing fraud.

To avoid this problem, Web browsers incorporate encryption technology that cloaks information and makes it difficult to get at. Encryption is the basic technique that the Web uses to guarantee information security.

The current encryption standard is called “Secure Sockets Layer” (SSL), supported both by Microsoft and Netscape, and incorporated in their browsers. An icon in the browser changes to indicate that SSL is active. When you make a transaction with SSL active, you can be fairly comfortable that the transaction is safe.

When you visit an SSL-secured site, the latest versions of Netscape Communicator and Microsoft Internet Explorer use a visual cue to tell you that the site is secure. For more information, see *How can I tell if a Web site is secure?*

NOTE: Guard Dog’s CheckUp lets you know if your Web browser is up-to-date. The latest browser versions usually offer an enhanced degree of security.

How can I tell if a Web site is secure?

Today, many sites use SSL to set up secure commerce on the Web. In addition to Web server security, the most common Internet browsers provide feedback about the security level of the site to which you are currently connected. For example, Netscape Communicator displays a lock icon in the lower left corner of the browser window. If the lock icon is broken, the site is not secure. If the lock symbol is not broken, the site is secure. In addition, if the lock symbol has a gold background, the site is using strong, 128-bit encryption.

Recent versions of Microsoft Internet Explorer and America Online browsers also display security information. For more information about how your browser indicates the security level of sites, refer to your browsers on-line help, or the printed documentation.

If SSL is so great, what is the problem?

SSL is affected by a couple of problems. One problem is that not everyone has an SSL-enabled server or browser. Some Web administrators don't want to use SSL because they have to pay for it, and it can also slow down server transactions. A more onerous problem that affects SSL is the way it is implemented. It turns out that some developers made incorrect assumptions about SSL, which means some older browser versions are less secure. The good news is that Microsoft and Netscape now coordinate their security efforts, which means a more secure, universal standard for Web security.

What about authentication?

Authentication is a method of assuring that both parties to an Internet transaction are who they claim to be. For example, if you get account balance information from your bank, you want to be sure that you are contacting the bank, and not some unauthorized entity. In addition, the bank wants to be sure that they are providing the information to you, and not just to a person who happens to know your bank account number.

Authentication usually entails entering a user ID and a password. To circumvent intercepted passwords and IDs, authentication employs encryption to scramble this information before transmitting it.

NOTE: Certificates are a Microsoft technology designed to guarantee a person's identity and Web site security. Personal certificates verify that you are who you claim to be. Web site certificates verify that a Web site is secure and what it claims to be (so Web sites can't falsify their identity). When you open a Web site that has a certificate, Internet Explorer checks if the certificate is correct. If the certificate is not OK, Internet Explorer warns you. Certificates are great, in theory. The problem is that they only establish a security standard—Web sites are free to choose to use certificates, or not.

How does encryption work?

The only way to keep a secret is if you do not tell anyone, and if you do not jot it down. If you need to share the secret, you can hide it within another message, and let the intended recipient know how to find it. Computer encryption hides messages by making the original data unintelligible. The intent is to garble the data for anyone for whom it is not intended: Having access to the encrypted data itself is useless.

The simplest encryption systems use letter shifting, in which a message is encrypted by shifting every letter *n* letters later in the alphabet. For example, say A is changed to B, and B to C, etc. As long as the recipient knows how you shifted the letters, they can easily decrypt the message by reversing the process. Of course, a brute force approach to breaking this sort of encryption would simply try all possible 26-letter combinations until the final message was retrieved—not a very strong method of encryption.

Computer encryption uses a much more difficult technique of hiding the message. Rather than a simple letter-shifting scheme, the original message is transformed by a mathematical algorithm. The algorithm uses a secret “key” to scramble the message, and the key is necessary to unscramble it. The key is similar to a house key: The more teeth a key has, the more difficult it is to pick the lock. Similarly, “strong” encryption uses keys with many “teeth”—in this case, bits of data.

There are two commonly used levels of encryption. The international standard is 40-bit encryption, but some sites in the United States use a higher level of 128-bit encryption. The number of bits indicates the length of the key used to encrypt data. The longer the key, the stronger and more secure the encryption.

On the Web, your browser works with secure Web sites to establish and manage the encryption that secures information. If your browser security options include the Secure Sockets Layer (SSL), which ensures data-transmission privacy, you should turn on this option to facilitate secure data transmission.

NOTE: Guard Dog’s CheckUp automatically checks your browser’s security level, and lets you know if you need to change it.

Security on the Web

One of the most exciting Web developments is the evolution of downloadable, executable programs. Java and ActiveX are two tools that help developers create programs that can “live” inside Web pages, and use your Web browser to automatically run over the Internet. Java allows Web pages to host small programs called “applets.” When Java-enabled browsers access a Web page containing Java, they automatically download and run the applets they find on the page. This is an intriguing development, since it makes it possible to download and run programs over the Web. Complete, Web-driven programs written entirely in Java are on the horizon. ActiveX is a similar technology, developed by Microsoft.

Java contains an internal security system that addresses security risks. ActiveX uses a different model, based on certificate authentication. Certificates contain information about who developed the ActiveX code. The idea here is that if you know who developed the code, it is safe to run it. Both security schemes offer a level of safety, but no one can yet promise that executable content is entirely safe.

Nasty applets

One possible security threat is a malign Java or Active X program that attacks your computer over the Web. A nasty applet might, for example, thwart Java security by circumventing its security model, and destroy data on your hard disk, or grab sensitive information from your hard drive. The latest browsers have done a good job of fixing these issues. As long as you are using the latest version of your browser you are protected. To date, there have been no legitimate reports of hostile Java or ActiveX harming anyone. However, there is no guarantee that an attack will not happen in the future.

Can I prevent programs from accessing the Internet?

You can use Guard Dog to specify the applications that are allowed to access the Internet from your computer. Obviously, your default Internet browser is one of these applications.

If the Guard Dog Gatekeeper is running in the background while you work on the Internet, each time an application tries to access the Internet a dialog box appears to ask if you want to allow this access once only, always, or never.

Computer viruses and the Web

A computer virus is a small computer program that automatically replicates itself and spreads from PC to PC. Viruses may infect programs, your hard drive, and even some document files that employ macros. Viruses do not infect data files, but they can create problems that prevent you from accessing your data. Viruses are not accidents—they are always created by computer programmers.

PC viruses are similar to biological viruses in that they:

- Are spread from host to host—the “host,” in this instance, is your PC.
- Are very good at reproducing themselves.
- Can wreak havoc in an infected host system.

Biological viruses have proven to be tenacious: modern medicine's success in fighting viral infection has, so far, been rather limited. Fortunately, PC viruses differ from biological viruses in that they are easier to combat, once they are identified.

Are viruses really that dangerous?

Bear in mind that your chances of contracting a PC virus are slim, and your chances of contracting a truly vicious virus even more so. The scariest viruses are malicious programs that intentionally corrupt or delete the data on your PC. More benign viruses might simply display a message on your monitor or make a strange sound, and then disappear. But even the most benign virus occupies some disk space, and many remain in memory, which can cause your PC to behave erratically or crash.

Types of viruses

There are three main types of viruses:

- **File or program viruses**: A program virus attaches itself to a specific program on your PC. Since many PC's share certain files in common (for example, the DOS program **command.com,** or the command "**dir**"**)**, which make these files tempting targets for virus programmers. Program viruses are dormant until you run the associated program.

- **Boot viruses (or Master Boot Record viruses)**: The boot sector of a disk is a physical location on the disk that contains information about the disk and the files it contains. All disks and drives have a boot sector, even if they aren't "bootable." A boot virus infects the boot sector of floppy disks and hard drives, and are activated when you access or boot from an afflicted disk.

- **Macro viruses**: Macro viruses are contained in document files, such as Microsoft Word or Excel files. These files can contain macros that can automate your work—but macros can also be written to do damage to your PC. Macro viruses are activated when you open an infected document file.

A final word should be said about hoax "viruses," which are not viruses in the strictest sense of the term. A hoax virus replicates a hoax, spread by misinformed (if well intentioned) e-mail claiming that if you download a certain file, or if you receive an e-mail with a certain subject line, you will infect your PC with a virus. E-mail messages are always safe; they are simple text files, and cannot contain viruses. Attachments to e-mail messages (an attachment is a file that a message sender attaches to a message—it is downloaded to your PC when you retrieve the message) can contain viruses. (If Email file access is turned on in Virus Sentry, Guard Dog automatically scans e-mail attachments before you open them.)

How can my PC become infected with a virus?

An important thing to keep in mind is that viruses are spread *only* when you run an infected application (or open an infected document file, in the case of macro viruses). A virus cannot travel over your telephone line and infect your PC on its own. You must first download or copy an infected application and then run the application in order to infect your PC with a virus.

That said, the only way to entirely avoid virus infection is to do nothing—don’t use the Internet; never download a file; never accept a diskette from someone else; never share Word or Excel files. Of course, this draconian “Robinson Crusoe” cure is unrealistic in today’s computing environment, where sharing data is the norm and accessing the Internet is an everyday occurrence.

NOTE: Guard Dog offers a virus scanner which is easy to use. It automatically scans your PC for signs of virus infection, and investigates suspect files before they have a chance of infecting your PC.

Viruses are spread when infected diskettes are shared between PCs, and when you download and run infected files from on-line services, bulletin boards, or the Internet. Another potential (but remote) route for virus transmission is when you access Web pages that use Microsoft ActiveX technology or Sun’s Java. Web pages that use ActiveX, for example, can automatically download programs to your PC, and these programs might be infected with a virus. Although there is no known case where ActiveX and Java have spread viruses, there is still a possibility— remote as it may be—for your PC to encounter a virus in this way.

A virus might be hidden in the next file you download, or on a diskette you borrow —even diskettes purchased at a store. Downloaded shareware is also a source of infection.

NOTE: Although Java and ActiveX are not, strictly speaking, viruses (they can’t spread and replicate), they can still harm your PC. Guard Dog’s default settings allow it to monitor all Java and ActiveX activity on your PC, and warn you before something potentially dangerous occurs.

Frequently asked questions about Internet privacy

What information do Web sites collect about me?

Web sites collect information about you in two major ways.

- First, you can provide the information yourself when you register software or respond to Internet questionnaires.
- Second, when you ask to be allowed access to the electronic version of a newspaper, or use a “shopping cart” to buy products on the Web, a cookie, described in “What are cookies and how are they used?” on page 69, might be written to your computer where it stores information, such as your user ID and password for the newspaper or the articles you bought with their quantity and price.

What information do companies get when I register products online?

Companies get only the information that you enter in the registration form when you register electronically. They do not get any information about your computer system, your use of your computer, or other stored information unless you provide it as part of the registration.

This information is used for the company’s marketing research and to send you information about new releases, other products, and so on. The information might be sold to other companies, just as mailing lists of magazine subscribers or mail order companies can be sold to others.

Some companies allow you to specify that you do not want to receive mailings or to have your name and address sold to other companies. If the company does not provide this option, you can enter false information to prevent mailings, either postal or electronic, from reaching you.

What are cookies and how are they used?

A cookie is a small file that contains data. The data in the cookie varies, depending on its purpose. Upon the request of a Web site, your Web browser stores cookies on your computer. Usually, cookies just contain information that enhances your Web experience. For example, when you use an Internet site to buy computer equipment, you may add items to a “shopping basket.” Information about the items you add to the shopping basket is stored in a cookie on your computer because the Internet browser cannot retain information that you entered in one Internet page when you switch to another Internet page. The cookie saves information about your purchases and allows the site to create a final order form for you.

Another example is the cookie that a Web store keeps on your computer, holding your user name and password so that you do not need to enter this information each time you connect to the site.

Some stores may use the cookie information to record each time you connect to the site, what pages you use, and whether you click any of advertiser banners. Reputable sites provide privacy information to tell you how the information that is gathered is used.

The above examples of cookies are clearly useful to you, at least in some way. However, other sites might download cookies just to collect information about your Internet use. These cookies are clearly not useful to you at all.

You can use the Guard Dog Cookie Blocker to control which cookies can be downloaded to your computer. For more information, see “What Cookie Blocker does” on page 35.

Sources for Internet privacy and security information

Finding out about Internet hoaxes

The United States Department of Energy—Computer Incident Advisory Capability

Lists and describes hoaxes, viruses, and miscellaneous security information.

http://ciac.llnl.gov/

More information about computer viruses

International Computer Security Association Anti-Virus Lab

http://www.ncsa.com/virus/

Describes viruses, virus alerts, as well as hoaxes.

Yahoo!'s virus page

Yahoo!’s virus page contains links to anti-virus software companies, Usenet virus newsgroups, and links to specific virus information.

Usenet virus FAQ

Contains a nicely organized compendium of information about viruses collected from Usenet virus newsgroups.

http://www.cis.ohio-state.edu/hypertext/faq/bngusenet/comp/virus/top.html

More information about security

Two good starting places for information about Web security is the on-line help for Netscape Communicator and Microsoft Internet Explorer.

National Institute of Health's Computer Security Information site

Good links to many security information sites.

http://www.alw.nih.gov/Security/security.html

Microsoft's Security site

White papers and descriptions of Microsoft's security efforts

http://www.microsoft.com/security/

More information about privacy

Electronic Freedom Foundation

http://www.eff.org/pub/Privacy/

Internet Privacy Coalition

http://www.privacy.org/ipc/

Product Support B

BEFORE YOU CONTACT McAfee Software for technical support, locate yourself near the computer with McAfee Guard Dog installed and verify the information listed below:

- Have you sent in your product registration card?
- Version of McAfee Guard Dog
- Customer number if registered
- Model name of hard disk (internal or external)
- Version of system software
- Amount of memory (RAM)
- Extra cards, boards or monitors
- Name and version of conflicting software
- EXACT error message as on screen
- What steps were performed prior to receiving error message?
- A complete description of problem

How to Contact McAfee

Customer service

To order products or obtain product information, contact the McAfee Customer Care department at (408) 988-3832 or write to the following address:

McAfee Software
3965 Freedom Circle
Santa Clara, CA 95054
U.S.A.

Technical support

Support via the web

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web (http://www.mcafee.com) a valuable resource for answers to technical support issues.

We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information.

Support forums and telephone contact

If you do not find what you need or do not have web access, try one of our automated services.

Table B-1.

World Wide Web	www.mcafee.com
CompuServe	GO MCAFEE
America Online	keyword MCAFEE

If the automated services do not have the answers you need, please contact McAfee at the following numbers Monday through Friday between 6:00 AM and 4:00 PM Pacific time for 30-day free support and between 6:00 AM and 8:00 PM for Per Minute or Per Incident support.

Table B-1.

30-Day Free Telephone Support	972-855-7044
Per Minute Telephone Support	1-900-225-5624
Per Incident Telephone Support	1-888-847-8766

McAfee training

For information about scheduling on-site training for any McAfee product, call (800) 338-8754.

Index

A

ActiveX controls 43
- deleting files 46
- protection against damage by 46
- scanning hard drives 46
- viruses and 68

alert messages 22
- Cookie Blocker 36
- File Guardian 47
  - ActiveX alert message 47
  - ActiveX delete alert message 48
  - drive format alert message 48
  - guarded file alert message 47
- Gatekeeper 43
  - any credit card number goes out 45
  - harmful site 44
  - Internet access 43
  - program starts up another program 44
- help for 22
- Identity Protector 38
- sounds for 29
- Virus Sentry 54
- Web Trail Cleaner 40

automatic actions 29

B

barking sounds 29

bookmarks 40

boot sector viruses 67

Browser Buddy
- adding a new password record 23
- dragging passwords from 24
- opening 23
- Password Manager and 23
- Search Filter and 41

browser history 40

C

cached files 40

CheckUp
- changing settings 32 to 33
- using 19

Cookie Blocker
- alert message 36
- Browser Buddy and 23
- described 35
- settings 37

cookies
- Browser Buddy 23
- defined 69

credit cards
- protecting with Gatekeeper 43
- protecting with Identity Protector 37

D

decrypting files
- using Scheduler 30
- using shortcut menu 21

deleted files, removing 30

direct sites 35, 37

diskettes
- boot sector viruses 67

dog barks 29

E

e-mail
- attachments and viruses 67
- messages and viruses 67

Emergency Disk
- creating during Interview 15
- scheduling reminder 31

encrypting files 25
  File Guardian and 46
  using Scheduler 30
  using shortcut menu 21
events, scheduling 29

F

file encryption 25
File Guardian
  ActiveX alert message 47
  ActiveX delete alert message 48
  alert message 47
  described 46
  drive format alert message 48
  encrypting and decrypting files 25
  guarded file alert message 47
  settings 49
files
  encrypting and decrypting 25
  protecting from ActiveX controls 46
  protecting with File Guardian 46
  removing deleted files 30
  scheduling encryption / decryption 30

G

Gatekeeper
  alert messages 43
  any credit card number goes out alert message 45
  described 43
  harmful site alert message 44
  Internet access alert message 43
  program starts up another program alert message 44
  settings 45
Getting Started manual
  described 5
Guard Dog
  See also alert messages; Protection Settings
  alert messages
  changing Protection Settings 27
  CheckUp 19
  help, described 5
  Home screen 17 to 18
  installing 8
  Interview, running 13
  Log 20
  manual, described 5
  new features 3
  password 16, 29
  shortcut menu 21
  sound effects 29
  splash screen 29
  system requirements 7
  taskbar icon 21
  updating 20
guarding files 25

H

hard drives, protecting 46
help
  alert messages and 22
  using 5
history files 40
hoax viruses 67
Home screen
  items on 17
  using 17 to 18

I

icon for Guard Dog 21
Identity Protector
  alert message 38
  described 37
  settings 39

indirect sites 35, 37

Internet connection, protecting 43

Internet privacy and security
- Guard Dog solutions 2

Interview 13 to 16
- creating an Emergency Disk 15

J

Java and viruses 68

K

kids *See* multiple users and passwords

L

Log 20

login names 50

logo screen 29

M

macro viruses 67

managing Web passwords 23

Master Boot Record viruses 67

menu, shortcut 21

messages *See* alert messages

modem 43

multiple users and passwords 29, 38

O

OCX 49

options
- CheckUp 32 to 33
- Preferences 29
- setting 27

P

Password Manager
- adding a new record using Browser Buddy 23
- adding record to 51
- deleting record 51
- described 50
- editing record 51

passwords
- activating and deactivating 39
- adding record to Password Manager 51
- adding with Browser Buddy 23
- Browser Buddy and 23
- creating for Guard Dog 29
- deleting Password Manager record 51
- dragging from Browser Buddy 24
- editing Password Manager record 51
- forgotten 16
- protecting Web site 51
- protecting Windows 46
- retrieving Guard Dog 16
- storing in Password Manager 50
- using for Guard Dog 16

personal information, protecting 37

Preferences settings 29

privacy threats 2

program viruses 67

programs, protecting 43

protecting
- credit cards 43
- files from ActiveX controls 46
- files with encryption 25
- Guard Dog 29
- hard drives 46
- Internet connection 43
- programs 43
- Windows password file 46

Protection Settings
- changing 27 to 31
- Cookie Blocker 37
- File Guardian 49
- Gatekeeper 45
- Identity Protector 39
- Password Manager 50
- Preferences 29
- Scheduler 29
- Search Filter 41
- Virus Sentry 54
- Web Trail Cleaner 41

Q

question mark button 22

R

report *See* Log

S

scanning for viruses 30

Scheduler 29
- adding an event 29
- editing an event 31
- file encryption 30
- removing an event 31
- virus checks 30

scheduling Guard Dog events 29

Search Filter
- Browser Buddy and 41
- described 41
- settings 41

search information 41

secure connection 37

security threats 3

settings
- CheckUp 32 to 33
- Cookie Blocker 37
- File Guardian 49
- Gatekeeper 45
- Identity Protector 39
- Scheduler 29
- Search Filter 41
- Virus Sentry 54
- Web Trail Cleaner 41

shareware and viruses 68

shortcut menu 21

slack space, wiping 30

sound effects 29

splash Screen 29

starting Guard Dog with Windows 29

T

taskbar icon 21

turning on / off
- barking sound 29
- Guard Dog monitoring 21
- splash screen 29

U

unsecure site 38

Update button, using 20

updates, scheduling reminder 31

updating Guard Dog and virus patterns
- using Scheduler 31
- using Update 20

URLs 40

username
- adding with Browser Buddy 23
- dragging from Browser Buddy 24

V

Virus Sentry
- alert message 54
- described 54
- settings 54

viruses
- ActiveX and 68
- e-mail attachments and 67
- e-mail messages and 67
- file and program 67
- hoax 67
- how dangerous? 67
- how spread 66
- Java and 68
- macro 67
- scheduling scans 30
- threats 3
- types of 67
- updating list of 20
- updating patterns with Scheduler 31
- who creates them 66

W

warnings *See* alert messages

Web password management 23

Web sites
- harmful 43
- storing login names and passwords 50

Web Trail Cleaner
- alert message 40
- described 39
- settings 41

Windows
- protecting password file 46
- starting Guard Dog automatically 29
- taskbar 21
- using help 5

wiping slack space 30