

What Guard Dog does

When you use [browse a Web site](#), you very likely wonder what kinds of information pass between your computer and the computers on the [Internet](#). You've probably heard that most of what goes on is good, but some things aren't, like [viruses](#) and [Trojan horse](#) programs.

Protecting the integrity of the data on your computer and guarding your privacy from intrusion by unauthorized programs designed to collect information about you are major concerns. CyberMedia Guard Dog is designed to protect your data and lets you take charge of how you use the Internet.

Guard Dog protects you in two basic ways:

- First, Guard Dog checks your computer for potential security risks and privacy issues and allows you to fix these problems before data is damaged or your privacy is compromised. A few of the things Guard Dog checks for:
 - Programs that have access to the Internet.
 - Sensitive data, such as financial files, and the programs that can access them.
 - Viruses that can damage the data on your computer or even go so far as to reformat your hard disk.
- [ActiveX](#) controls and [Java applets](#) that may or may not perform dangerous actions on your computer.
- Second, Guard Dog lives up to its name by standing guard and alerting you to potential harmful events that threaten your privacy and security. Some of the things that will trigger a Guard Dog alert:
 - Unwarranted intrusion from other sources on the Internet.
 - Programs on your computer that pass sensitive data to other sites.
 - Web sites that send [cookies](#) to your computer as you use the Internet.

See the following topic for more information about privacy and security.

[Some things you should know about privacy and security](#)

Guard Dog's extensive suite of protection features operate on two levels:

Features that you can use immediately:

- Checking the security on your computer.
- Checking files for viruses.
- Cleaning your browser by ridding it of all traces of your Web browsing history.
- Updating Guard Dog with the latest protection technology from CyberMedia.
- Running the Interview to change your privacy and security preferences.
- Setting up password-protection for Guard Dog.

Features that work while you use your computer::

- Monitoring the programs on your computer that can connect to the Internet. If an unauthorized program tries to connect, Guard Dog alerts you.
- Protecting your e-mail and critical system files from tampering by unauthorized Trojan horse programs.
- Preventing others from snooping in your Internet browser files and compromising your privacy.
- Blocking unauthorized Internet-based programs from gaining access to personal data.
- Alerting you to the presence of a virus in new files, such as files that are downloaded or received by e-mail.

The suite of features included in Guard Dog represents the minimum protection that any Internet user should have. As CyberMedia improves the product, you can use the Update feature to keep Guard Dog up-to-date with the latest product improvements.

See the following topics for information about Guard Dog's password-protection, privacy, security features.

[About Guard Dog Preferences](#)

[About Scheduler](#)

[About Cookie Blocker](#)

[About Identity Protector](#)

[About Web Trail Cleaner](#)

[About Search Filter](#)

[About Gatekeeper](#)

[About Password Manager](#)

[About Virus Sentry](#)

How Guard Dog works

CyberMedia designed Guard Dog to ensure that you can use all aspects of the [Internet](#) without worrying that your privacy or computer security will be compromised. Guard Dog attempts to protect you as transparently as possible without a lot of technical jargon and detail.

Guard Dog simplifies things by:

- Conducting a preliminary Interview

The first time you run Guard Dog, you interact with the program by answering a few questions. Guard Dog uses your answers to determine how best to ensure your particular security and privacy needs. When you complete the Interview, Guard Dog is ready to protect your computer. If your security needs change, you can run the Interview again.

See the following topic for more information about determining your protection requirements.

[Responding to Interview questions](#)

- Monitoring your computer habits

As you use the program, Guard Dog may ask additional questions. Guard Dog is learning about how you use your computer and the Internet. Although these questions may be a little disruptive, you shouldn't have to answer too many of them after the first few times you use your computer. We hope you can be patient and carefully answer the questions posed by Guard Dog.

If you routinely find that Guard Dog warns you incorrectly, then Guard Dog is not customized properly for you. To remedy this situation, you can either answer the Interview questions again or change Guard Dog settings directly in the **Protection Settings** dialog box.

See the following topic for more information about the Internet Guardian Properties.

[Understanding Guard Dog Privacy Settings](#)

- Running Guard Dog in the background

Part of Guard Dog runs unobtrusively in the background protecting your computer while you use it. The Guard Dog icon in the system tray in the right corner of the Windows taskbar as an indication that it is on the job. However, when Guard Dog detects a security threat, it alerts you by displaying an alert dialog box in the foreground containing options for handling the situation.

See the following topic for more information about responding to alerts.

[Responding to Guard Dog Alerts](#)

Some things you should know about privacy and security

With the explosion of interest in the Internet and the expansion of the [World Wide Web](#) to offer goods and services in exchange for money, security is becoming an important issue. Business transactions must be protected on both sides—the buyer and the seller. The problem with conducting business over the Internet is easy to define. While it is relatively easy to set up a Web site to display and sell things, it is not so easy to develop mechanisms to ensure the security of the information that must be passed back and forth to accomplish any type of transaction. Added to this is the presence of people (called hackers) who have the skills, the software, and the inclination to monitor transactions and snare important data like credit card and bank account numbers.

However, there is hope. An encryption technology called “Secure Sockets Layer” has been incorporated into Microsoft Internet Explorer and Netscape [browser](#) software. When you choose to use this technology, an icon appears in the browser to indicate SSL is active; and when you do use it, you can be fairly certain that your transaction is safe.

Encryption is great, but again, we are faced with a couple of problems. First, not all servers and browsers are SSL-enabled. SSL software adds to the investment cost associated with the server and can also slow down server transactions. Second, Microsoft and Netscape did not coordinate their security efforts meaning that although neither company’s browser is immune to security problems, they are not necessarily the same ones. You could very easily be at a loss to assess your security risk and have to rely on flipping a coin to determine which browser is the safer. However, the companies are attuned to the risks and pitfalls involved in implementing security measures and are working to correct their problems.

Secure transactions are only part of the problem. Once Web servers receive information, they must be able to keep it safe. In a large network, one in which a Web server is just one of several types of server, the network administrator tries to isolate the Web servers from other mission-critical servers. However, some Web applications interact with data stored on other servers, thus opening a door to potentially sensitive data. Hackers target Web servers because the technology to secure these servers is still being developed. A security technology called a “firewall” can control unauthorized access to sensitive data, but it must be properly maintained. Even in the most well kept systems, a firewall cannot protect certain services.

From a user perspective, there are one or two ways to tell if you can safely transmit information to a Web Site.

First, most business-oriented Web sites do implement server security and will notify you that you are using a secure connection. If the site is not secure, you are warned that you are sending information to a non-secure site and are given the option to continue. Second, most browsers are intelligent enough to detect the security level of the site you are connected to and will display this information.

It is always wise to use every security measure available to you because the world is filled with less than honest people who will take advantage of the unprotected. Microsoft and Netscape are working diligently in the security field to remedy security leaks in existing Internet products and to develop advanced solutions to prevalent security issues. To take advantage of their latest developments, keep your browser software up-to-date by running Guard Dog frequently.

Protecting your private personal information while using the Internet

Protecting the integrity of the data on your computer and guarding your privacy from intrusion by unauthorized programs designed to collect information about you are major concerns as you use the [Internet](#). Guard Dog provides a collection of privacy features designed to protect your sensitive personal information particularly as you [browse](#) the Internet.

These features include:

- **Cookie Blocker**

[Cookies](#) can help a [Web site](#) better serve you by using information it has previously obtained and stored on your computer. For example, cookies can allow your favorite merchandising site to display custom information for you each time you visit, or allow a password-protected Web site to retrieve your password so that you don't have to enter it each time you visit the site.

Because you have no control over what is being tracked or who is collecting information about you, cookies also represent a threat to your privacy. Cookie Blocker lets you control who sends and retrieves cookies on your computer. Thus, you can enjoy the benefits that cookies offer at your favorite Web site while blocking new cookies from other sites.

- **Identity Protector**

Guard Dog lets you specify certain types of personal information for it to keep an eye on. You can enter your name, address, e-mail address, as well as bank account and credit card numbers. Guard Dog will alert you when an application tries to send anything that you have entered in Identity Protector over the Internet.

- **Web Trail Cleaner**

Guard Dog keeps track of your browsing activities. After you exit the Internet, Web Trail Cleaner removes the Internet history files and deletes files from the browser [cache](#). This can be very useful to maintain privacy and security in environments where users share computers.

- **Search Filter**

Guard Dog keeps an eye on certain types of activity as you browse the Internet. For instance, you may enter your e-mail address at a site. This information is recorded and correlated with cookies allowing certain Web sites to build databases containing information about you and your interests. You may not want this information to be collected. When Search Filter is turned on, your important information stays where you put it.

Creating a secure computing environment

Protecting the integrity of the data on your computer from intrusion by unauthorized programs designed to collect information about you are major concerns as you use the [Internet](#). Guard Dog provides a collection of privacy features designed to protect your sensitive personal information especially as you [browse](#) the Internet.

These features include:

- Gatekeeper

Gatekeeper keeps a watchful eye over your computer and what goes on as you use the Internet. Gatekeeper acts as your safety net warning you when you are about to connect to [Web sites](#) that contains harmful content such as [ActiveX](#) controls or [Java applets](#). Other programs that you install on your computer can come from many sources. Some may or may not be entirely reliable. You really can't tell what a program is going to do until you install and use it. Something that is seemingly innocent may be designed to look for certain types of information on your computer and use the Internet to transmit this information to another computer.

Gatekeeper alerts you if an unauthorized program tries to connect to the Internet or when information that is being protected in Identity Protector is sent out over the Internet.

See the following topic for more information about the Gatekeeper.

[About Gatekeeper](#)

- File Guardian

File Guardian's primary purpose is to protect sensitive or critical files on your computer by allowing you to specify which applications have access to them. File Guardian automatically protects your e-mail files so that only the mail application can use them. You may want to add other files to the Guard Files list, such as financial files, thus ensuring that only the application that you used to create these files has access to them.

A second important File Guardian function is to alert you when it detects potentially harmful events such as ActiveX scanning your hard drive, or a [Trojan horse](#) program reformatting your disk drive.

See the following topic for more information about the Browser Buddy.

[About File Guardian](#)

- Password Manager

Can you remember the password and user name for every protected [Web site](#) that you visit? If you have committed them to paper, do you remember where you put the list and do you have a safe place to keep it?

If you let Guard Dog manage your passwords you won't have to worry about the answers to these questions. To avoid typing your user name and password each time you visit a password-controlled you can drag and drop this information from the Browser Buddy to the appropriate boxes on login screen.

See the following topic for more information about Password Manager.

[About the Password Manager](#)

See the following topic for more information about the Browser Buddy.

[About the Browser Buddy](#)

Protecting important data from virus infection

[Viruses](#) are easy to come by especially if you download data from [Web sites](#). By constantly scanning new files for viruses, Virus Sentry can greatly reduce the risk of virus infection by removing viruses before they can do damage.

You have complete control over Virus Sentry. You can set it up to run automatically in the Virus Sentry Protection Settings page, or you can customize CheckUp to run virus checks as needed.

CyberMedia works constantly to identify viruses and find cures for them. CyberMedia places information about known viruses in a virus pattern file. As new viruses are identified the pattern file is updated with the new information. You can load the latest virus pattern file by using Guard Dog's Update feature.

See the following topics for more information about Virus Sentry.

[Determining what CheckUp checks](#)

[About Virus Sentry](#)

See the following topic for more information about the Update feature.

[Using Update](#)

Using the features in the Guard Dog Home screen

The Guard Dog Home screen is your entry point into the world of Guard Dog's protection and security features.

From here you have access to the following features:

- **CheckUp**

When you run Check-Up, Guard Dog gives your computer a comprehensive inspection for potential security problems and privacy issues. When Guard Dog finds problems, Guard Dog creates a list and displays the list on the CheckUp Found screen. You can select a problem and Guard Dog will display an additional screen containing a description of the problem and a recommendation about how to fix it. If you fix a problem and don't like the result, Guard Dog lets you Undo the fix.

See the following topics for more information about CheckUp

[Using CheckUp](#)

[Determining what CheckUp checks](#)

- **Update**

CyberMedia works constantly to improve Guard Dog. Most of these improvements—called updates—are available on the CyberMedia [Web site](#). The Update feature uses CyberMedia's Oil Change technology and your [Internet](#) connection to search for any available updates to Guard Dog software. You can use Oil Change to download and install them. If you don't have Oil Change installed, you won't be able to use the Update feature.

See the following topic for more information about Update.

[Using Update](#)

- **Log**

You can see what Guard Dog has been doing to protect your security and privacy using the **Log** feature. Look in the Guard Dog Action column to find out what Guard Dog has done the look in the Type column to see which Guard Dog feature performed the action.

Tip

To see the entries in the Guard Dog Actions and Type columns displayed alphabetically, click either column heading.

See the following topic for more information about the Log.

[Using the Guard Dog Log](#)

See the following topic for more information about the Browser Buddy

[About the Browser Buddy](#)

Using CheckUp

The Check-Up feature gives your computer a comprehensive inspection for potential security problems and potential privacy issues. Guard Dog summarizes the problems that CheckUp identified and displays them in the CheckUp Found screen.

Guard Dog also identifies security issues and actions that may have occurred recently on your computer so that you can deal with these as well. When Guard Dog completes a Check-Up, you can be confident that Guard Dog will continue to maintain the privacy and security of any sensitive data on your computer.

Specifically, you can use Check-Up to ensure that:

- The programs on your hard disk are free of [viruses](#).

- Your e-mail and critical files are being protected.

- Private information has been removed from your browser's history and cache folders.

- Your security settings make sense for you.

- You are comfortable with your recent handling of alerts.

- No one else has changed your security settings without your knowledge.

How do I perform a CheckUp?

▶ Click **CheckUp** on the Guard Dog home screen.

Guard Dog displays a second screen that lists the checks and provides progress information as it performs each one.

See the following topic for information about CheckUp.

[Determining what CheckUp checks](#)

[Responding to CheckUp Found](#)

Using Update

CyberMedia works constantly to improve Guard Dog. Most of these improvements—called updates—are available on the CyberMedia [Web site](#). The Update feature uses your Oil Change to search for any available updates—including updated [virus pattern files](#)—to Guard Dog software, downloads them and installs. If you don't have Oil Change installed, you won't be able to use the Update feature.

A limited version of Oil Change is provided on the Guard Dog CD. If you didn't install Oil Change when you installed Guard Dog, you can do so at anytime simply by placing the CD in the CD-ROM drive on your computer and following the instructions on the installation screen.

How do I update Guard Dog?

- ▶ Click **Update** on the Guard Dog Home screen. Guard Dog displays the Oil Change screen as it connects to the CyberMedia Web site to check for updates. If an update is available, Guard Dog downloads and installs it automatically for you.

Using the Guard Dog Log

To keep an eye on what Guard Dog is doing, check the **Log** from time to time. Guard Dog categorizes the actions that it has taken and presents the data in a list format. You can get rid of the information in the log by clicking **Clean**.

How do I print or clear the Log?

- 1 Click **Log** in the main Guard Dog screen.
- 2 To print a copy of the Log, click **Print** in the Guard Dog Log screen. Guard Dog will send the Log to your default printer.
- 3 To delete information from the Log, click **Clear** in the Guard Dog Log screen.

Tip

To see the entries in the Guard Dog actions and Type columns displayed alphabetically, click either column heading.

Using Guard Dog Options

You can control how Guard Dog works by using the settings available in the Options menu. You can change:

- **Protection Settings:** Guard Dog's privacy and security settings are contained in Protection Settings pages. This menu selection offers you access to the Protection Settings pages where you can add, change or remove setting information.

See the following topic for more information about Protection Settings.

[Understanding Guard Dog Protection Settings](#)

- **Customize CheckUp:** You can control what Guard Dog checks by making selections in the Customize Guard Dog screen.

See the following topic for more information about Customizing CheckUp.

[How do I customize CheckUp](#)

- **Interview:** This menu selection allows you to run the Interview if you want to change any of the information that you originally entered.

See the following topic for more information about the Interview.

[Responding to Interview questions](#)

How do I access the Guard Dog Options menu?

- ▶ The Options menu is available at the top of most screens.

Getting Help

Help is available in several forms. You can access Help from the Guard Dog Home screen and during the Interview if you want more information you can press **F1** to receive help for the page that you are working on. If you are fixing problems that Guard Dog identified during a CheckUp, you can get help on a specific screen by clicking **Help**, then clicking **Help for this screen**.

How do I access Guard Dog's Help system?

- 1 Click **Help** on the menu bar at the top of the screen.
- 2 Click **Help topics** to access the Help system, or click **Help for this screen** to receive more information about the screen you are looking at.
- 3 You can access the Help contents from the Guard Dog pop-menu. Right-click the Guard Dog icon and click **Help**.

See the following topic for more information about the entries on the Help menu.

[About the Help menu](#)


Responding to Interview questions

Whenever you use a security monitoring application on your computer, you must strike a balance between the amount of security you need and the impact that the monitoring has on the performance of your computer. To make these decisions easier, Guard Dog uses its Interview feature to ask questions about how much protection you need. You can use Guard Dog's recommendations to guide your selections. If you want more information about the page, press **F1** on your keyboard. After you finish answering the questions, Guard Dog uses your answers to automatically configure itself to fit your needs.

How do I restart the Interview?

- ▶ Click **Options** at the top of the Guard Dog Home screen and select **Interview** from the menu.

Tip

You can inspect or modify the settings that Guard Dog has selected for you in the Protection Settings dialog box. To open Protection Settings, right-click the Guard Dog icon  in the system tray on the Windows taskbar and select **Protection Settings** from the pop-up menu. Or, on the Guard Dog Home screen, click **Options**, and select **Protection Settings** from the menu.

See the following topic for more information about determining how much protection you may need.

[Understanding Guard Dog Privacy Settings](#)

Understanding Guard Dog Protection Settings

Guard Dog allows you to determine levels of privacy and security using a series of configurable options called Protection Settings. A part of Guard Dog is always on duty in the background to protect your computer's data and your privacy based on the choices you make. Guard Dog displays settings on a series of Protection Settings pages containing check boxes, list boxes, buttons, and other controls that you can use to enter settings.

See the following topics for more information about Options.

[Using Guard Dog Options](#)

[How do I access the Guard Dog Options menu](#)

The Protection Settings pages are organized in four categories:

- **Preferences**—The Preference category contains two Protection Settings pages:
 - Preferences Protection Settings page**—The settings on this page let you control Guard Dog's general behavior such as when it loads, how it alerts you whether a password is required to run the Guard Dog program. If your computer is equipped with a sound card, Guard Dog can provide an audible alert.
 - Scheduler Protection Settings page**—The settings on this page lets you set up Guard Dog to perform certain, time consuming tasks, like virus scans, at convenient times.

See the following topics for information about changing the settings on these Protection Settings pages.

[About Guard Dog Preferences](#)

[About Scheduler](#)

- **Privacy**—The Privacy category contains three Protection Settings pages:
 - Cookie Blocker**—The settings on this page let you set up Guard Dog to accept or reject [cookies](#) as you browse the Internet. You can choose how to deal with cookies from [direct](#) and [indirect](#) Web sites. When you first visit a site and decide whether to accept or reject a cookie, Guard Dog adds the site to the Allowed or Rejected sites list. By doing this, when you revisit a site, Guard Dog checks the lists and accepts or rejects the cookie without bothering you.
 - Identity Protector**—The settings in this page let you enter specific personal information for Guard Dog to guard. Guard Dog scans the files and folders on your computer to determine if they contain any of this personal and financial information. When Guard Dog locates these files, it asks you if you want to add these files to the list of files File Guardian monitors.
 - Web Trail Cleaner**—The settings on this page let you determine whether to delete Web Trail Cleaner deletes Web files automatically or prompts you each time you close your browser.
 - Search Filter**—As you browse the Internet, information about you can be passed from Web site to Web site. For instance, you may enter your e-mail address at a site. This information is recorded and correlated with cookies allowing certain Web sites to build databases containing information about you and your interests. You may not want this information to be collected. When Search Filter is turned on, your important information stays where you put it.

See the following topics for information about changing the privacy Protection Settings.

[About Cookie Blocker](#)

[About Identity Protector](#)

[About Web Trail Cleaner](#)

[About Search Filter](#)

- **Security**—The Security category contains three Protection Settings page:
 - Gatekeeper**—The settings on this page help you set up Gatekeeper to stand watch over your computer. Gatekeeper acts as your computer's safety net and warns you when it detects certain potentially harmful activity such as a sending credit card numbers out over the Internet or connecting to a [harmful Web site](#) .
 - File Guardian**—The settings on this Protection Settings page help you set up File Guardian to protect sensitive or critical files on your computer. You can also specify the types of warnings that File Guardian provides when potential harmful activity takes place, such as an unauthorized program trying to access a file that File Guardian is protecting. File Guardian can automatically protect your e-mail files so that only the mail application can use them. You may want to add other files to the Guarded Files list, such as financial files, thus ensuring that only the application that you used to create these files has access to them.
 - Password Manager**—To avoid typing your user name and password each time you visit a password-controlled [Web site](#), enter you user names and passwords in Password Manager. When you visit the site, you can drag and drop this information from the Browser Buddy to the appropriate boxes on login screen.

See the following topics for information about changing the settings on these Protection Settings pages.

[About Gatekeeper](#)

[About File Guardian](#)

[About Password Manager](#)

See the following topic for information about Browser Buddy.

[About Browser Buddy](#)

- **AntiVirus**—The AntiVirus category contains one Protection Settings page.
 - Virus Sentry**—The settings on the Virus Sentry Protection Settings page lets you set up Guard Dog's AntiVirus protection by specifying what to check, when to check, what not to check and what to do when a virus is found.

See the following topic for information about changing the settings on this Protection Settings page.

[About Virus Sentry](#)

Determining what Guard Dog checks

After completing the Interview, you'll want to find out how your computer may be at risk. CheckUp examines your computer for privacy, security, and virus problems based on the information you provided during the Interview and 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.

You can easily control what Guard Dog checks by rerunning the Interview. Guard Dog also stores the Interview settings in Protection Settings pages which you can access from the Guard Dog Home page. You can customize these settings to ensure that Guard Dog is the best job possible.

How do I customize CheckUp?

Click **Options** in the Guard Dog Home screen and click **Customize Settings**. In the left side of the screen, select the box by the check you want Guard Dog to perform.

If you reduced the level of protection, you should run CheckUp on a more frequent basis.

Tip

When you roll your mouse pointer over an item in the check list, a brief description of the check appears in the More Information box on the right. For more detailed information about each check, see the following description.

To check for general security concerns, you can select:

- **Emergency Disk Check**—Guard Dog checks to determine if you have created an Emergency Disk and if the information on the disk is up-to-date.

See the following topic for more information about Emergency Disk.

[About Emergency Disk](#)

- **Guard Dog Updates Check**—CyberMedia continually improves Guard Dog and places these improvements—called updates—on the CyberMedia Web site. If you select Guard Dog Updates Check, Guard Dog launches Oil Change which you can use check for program updates for Guard Dog as well as new [virus pattern](#) files. You can use Oil Change to locate, retrieve and install any available updates.

See the following topic for more information about the Update feature.

[Using Update](#)

- **Browser Version Check**—Microsoft and Netscape also improve their browser software and provide updates on their Web sites. You should keep your browser software up-to-date in order to take advantage of the additional security features that the browsers provide.

To safeguard your privacy, you can select:

- **Identity Protector Check**—Guard Dog scans files on your computer to determine if they contain any of the personal and financial information that you entered in Identity Protector either during the Interview or directly in the Identity Protector Protection Settings page. Guard Dog asks you if you want to add these files to the list of files File Guardian monitors.

See the following topics for more information about File Guardian and Identity Protector.

[About File Guardian](#)

[About Identity Protector](#)

- **Cookie Manager Check**—Guard Dog checks your computer to see if any [cookies](#) have been left behind after you closed your Web [browser](#).

See the following topic for more information about Cookie Blocker.

[About Cookie Blocker](#)

- **Search Filter Check**—When you delete files and folders from your hard drive, the data doesn't disappear. It remains on the disk and is overwritten. Guard Dog identifies this data and gives you the opportunity to remove it completely.

See the following topic for more information about Search Filter.

[About Search Filter](#)

- **Web Trail Cleaner Check**—Guard Dog determines if your browser has left any Web files on your computer.

See the following topic for more information about Web Trail Cleaner.

[About Web Trail Cleaner](#)

To create a secure computing environment, you can select:

- **Gatekeeper**—Guard Dog determines two of things when you select Gatekeeper:

Which programs on computer have unrestricted access to the [Internet](#).

Security level of the Microsoft Internet Explorer browser if you have it installed

See the following topic for more information about Gatekeeper.

[About Gatekeeper](#)

- **File Guardian**—Guard Dog checks for e-mail files (Microsoft Outlook, Netscape, Eudora, and so forth) and financial files (Quicken and MS Money). If it finds any of these types of files, Guard Dog determines if the files are protected by File Guardian. If they aren't Guard Dog asks you if you want to add them to the Guarded files list.

See the following topic for more information about File Guardian.

[About File Guardian](#)

- **Password Check**—Guard Dog determines whether any shared folders on your computer do not have passwords assigned

to them.

To keep the data in your files safe from virus infections, you can select:

- **Virus Sentry**—Guard Dog scans the files on your computer for viruses. You can select which folders to check.

See the following topic for more information about Virus Sentry.

[About Virus Sentry](#)

See the following topics for more information about CheckUp.

[Using CheckUp](#)

[How do I perform a CheckUp](#)

Responding to CheckUp Found

Guard Dog compiles a list of the problems and issues that it finds during a CheckUp. These problems appear under the Security, Privacy, and AntiVirus headings on the CheckUp Found screen. When you select a problem, you can perform the following actions:

- **Fix**—Click **Fix** to tell Guard Dog what action to take to solve a problem. Guard Dog displays a second screen containing important information about the problem and recommendations about how to fix the problem.
- **Undo Fix**—To identify a fixed problem, Guard Dog places a check by the problem on the CheckUp Found screen. If you aren't satisfied with the solution, you can return to the previous settings. Select the problem on the CheckUp Found screen and click **Undo Fix**.

Tip

If you want even more information about a problem, select a problem on the **CheckUp Found** screen and click **Fix**. When the **Fix** screen appears, click **Help** then click **Help on this screen**.

Understanding Guard Dog Security features

After completing the Interview, you'll want to find out how your computer may be at risk. CheckUp examines your computer for privacy, security, and virus problems and 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.

To create a secure computing environment, you can select:

- **Gatekeeper**–Gatekeeper stands watch over your computer and warns you when it detects certain potentially harmful activity such as a sending credit card numbers out over the Internet or connecting to a harmful Web site.

See the following topic for more information about Gatekeeper.

[About Gatekeeper](#)

- **File Guardian**–File Guardian's primary function is to protect sensitive files by allowing you to specify which programs can use these files. File Guardian can automatically protect your e-mail files so that only the mail application can use them. You may want to add other files to the Guarded Files list, such as financial files, thus ensuring that only the application that you used to create these files has access to them. A second major function of File Guardian is to monitor activity on your computer and warn you when potentially harmful activity, such as a program that tries to reformat your hard drive, takes place.

See the following topic for more information about File Guardian.

[About File Guardian](#)

- **Password Manager**–Password Manager creates a safe environment to store the passwords and user names that you use to log on Web sites. If you let Guard Dog manage your passwords you won't have to remember each the password or worry about trying to find the paper that you may have written it down on. To avoid typing your user name and password each time you visit a password-controlled you can drag and drop this information from the Browser Buddy to the appropriate boxes on login screen.

See the following topics for more information about Password Manager and Browser Buddy.

[About Password Manager](#)

[About Browser Buddy](#)

To keep the data in your files safe from virus infections, you can select:

- **Virus Sentry**– A [virus](#) at the very least can be a nuisance and at its worst can destroy valuable data on your computer. When you select Virus Sentry, Guard Dog check for viruses based on the settings you enter on the Virus Sentry Protection Settings page.

See the following topic for more information about Virus Sentry.

[About Virus Sentry](#)

About the Browser Buddy

Browser Buddy is a convenient way to get a summary of [cookie](#) activity. Keep it open as you browse [Web sites](#) to keep an eye on cookie activity.

In the Statistics box, you can choose:

- All Web Sites—displays the total number of cookies for all the Web sites you visit.
- Local Web Site—displays the total number of cookies that the Web site you are currently connected to.

Based on the selection you made in the Statistics box, you can get the following information:

- **Cookies Allowed**—Displays the total number of cookies for the Web site you selected in the Statistics box.
- **Cookies Blocked**—Displays the total number of cookies that were blocked for the selected Web site you selected in the Statistics.
- **Search Filter**—Displays the total number of times Guard Dog stopped your information from being sent to an [indirect](#) Web site.
- **Password Manager**—To avoid typing your user name and password each time you visit a password-controlled Web site, you can drag and drop this information from the Browser Buddy to the appropriate boxes on a login screen.

How do I access Browser Buddy?

On the Windows taskbar, right-click the Guard Dog icon



and click Browser Buddy in the pop-up menu. Click the Close icon (x) in the upper right corner of the dialog box to

How do I add a user name and password in Browser Buddy?

- 1 In Browser Buddy, select **Add New Entry** from the **Current Web Site** 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 **User ID** box, type the name by which you identify yourself to the Web site. On the Web site, this may correspond to Member ID, Member Name, Login ID, or Login Name, and so on.
- 4 In the **Password** box, type the password that confirms your identity. (Your password appears as a series of asterisks (*), one asterisk for each character in your password.)

5 Click **OK**.

How do I access the passwords stored in Browser Buddy?

- 1 In Browser Buddy, select the site name if it doesn't appear automatically in the **Current Web Site** list.
- 2 Drag your login ID or password from the Password Manager box to appropriate field in your Web site's login form. The text appears in the field. (Your password appears as a series of asterisks (*), one asterisk for each character in your password.)
- 3 Continue logging in as usual to the Web site.

About Emergency Disk

During the Interview, Guard Dog asks if you want to create an Emergency Disk on which Guard Dog saves the important, protected data, as well as a program that allows you to start your PC in DOS mode. If disaster strikes, you can restore Guard Dog settings from the disk.

Guard Dog can remind you to update the data on the Emergency Disk. Set the frequency of this reminder in the in the Scheduler. See the following topics for information about Emergency Disk reminders.

[About Scheduler](#)

[Respond to an Emergency Disk reminder alert](#)

Tip

You will need three 3.5" floppy disks for Guard Dog to use.

How do I create an Emergency Disk?

- 1 Click **Options** on the main Guard Dog home screen and click Interview.
Use the **Next** arrow to locate the **Emergency Disk** screen.
- 2 Insert a floppy disk in your computer's floppy drive and click **Create Emergency Disk**.
The wizard will help you with the process.

About the pop-up menu

Because you may want to work with Guard Dogs features without starting the Guard Dog program, some of the more frequently used features have been added to an easily accessible pop-menu. From the pop-up menu you can select:

- **Run Guard Dog**–Starts the program.
- **Browser Buddy**–Opens Browser Buddy.
- **Protection Settings**–Opens the **Protection Settings** dialog box where you can access the Protection Settings pages associated with Guard Dog settings.
- **Help**–Starts the Guard Dog program Help system and displays the contents.
- **Encrypt File Guardian files**–Adds [encryption](#) to files that you have selected for encryption in File Guardian's Guarded File list.
- **Decrypt file Guardian files**–Removes encryption from files making the data readable.
- **Exit**–Closes the Guard Dog program and removes it from your computer's memory. When you choose Exit, Guard Dog will no longer be on guard protecting your privacy and safeguarding the security of data on your computer.

How do I access the pop-up menu?

- ▶ Right-click the Guard Dog icon



in the system tray.

About the Help menu

If you are in doubt about how to use any of Guard Dogs features, use the Help menu to answer you questions. You can select:

- **Help Topics**–Gives you access to the complete Guard Dog Help system including the Contents, Index, and Find. Click a book in the Contents to display the titles of the topics beneath the book. Click a topic title to display the help topic associated with the title.
The Help system uses standard Windows Help navigation buttons, including **Help Topics** to return from a topic to the table of contents, **Back** to return to the topic you just reviewed, **>>** and **<<** to browse forward and backward through all the topics in the Help system.
- **Help on this screen**–Gives you access to a help topic containing information that has been tailored specifically for the screen that you are viewing. Press **ESC** on your keyboard to close the topic.
- **How Guard Dog works**–This selection gives you access to the Guard Dog video which introduces you to Guard Dog and its features.
- **CyberMedia on the Web**–This selection opens your [browser](#) and gives you access to the CyberMedia Web site where you can get the latest information for all CyberMedia products.
- **Guard Dog on the Web**–This selection opens your browser and connects to the Guard Dog Home page on the CyberMedia Web site where you can get the latest Guard Dog information.
- **FAQs**–CyberMedia's support team is committed to helping you get the greatest benefit from using Guard Dog, and to this end, they have made a list of the popular questions that they answer about Guard Dog. This selection opens your browser and give you access to the Frequently Asked Questions page on the CyberMedia Web site.
- **Report a problem**–Got a problem with Guard Dog? This selection opens your browser and gives you access to an e-mail form in which you can enter your complaint. Your e-mail will be sent to CyberMedia Support.
- **Virus Encyclopedia**–If you are interested getting details about any virus that CyberMedia has identified, this selection gives you access to a Help file which contains this kind of information. Click the Index tab and select the name of your virus from the alphabetical list.
- **About Guard Dog**–If you call CyberMedia Support, a technician may ask you which version of Guard Dog you have installed. This selection opens your browser and displays a page containing version and copyright information.

To tell Guard Dog what features to use, select or clear check boxes to the left of the feature name in the left pane of the dialog box. Click the name of the feature in the left pane, to display its configuration options in its Protection Settings page in the right pane

Restores all option settings for all protection features—except in Identity Protector and Password Manager—to the initial settings shipped with Guard Dog. When you restore your default settings, Guard Dog does not change which protection features (such as Scheduler or Cookie Blocker) are turned on or off.

Close the **Protection Settings** dialog box without saving any changes that you made to your settings.

Saves any changes you have made on any of the Protection Settings pages and closes the **Protection Settings** dialog box.

Preferences Protection Settings

You can control basic Guard Dog features and actions by selecting the options on the Preferences Protection Settings page.

Provides Information about the settings on this page and what they control.

Select the way that you want Guard Dog to work when Windows starts.

Displays the CyberMedia splash screen while Guard Dog is loading into your computer's memory.

Starts up the monitoring part of the Guard Dog program each time you start Windows.


You can control access to Guard Dog by assigning password protection to the Guard Dog program. You may have done this during the Guard Dog Interview. If that is the case, you can change the password here. If you didn't assign a password, you can do so now. It is wise to assign a password to Guard Dog because it provides an extra layer of protection between your sensitive private data and anyone else who might be using your computer.


Requests the Guard Dog password each time you start Windows.


If you haven't created a password or if you want to change an existing password, click **Change Password**.


Creates a new Guard Dog password or changes the existing password.


As Guard Dog monitors your computer, the program can warn you of impending situations that may be harmful to the data. If you have a sound card installed, Guard Dog can provide an audible alert in addition to the standard visual alert box. You can control these audible alerts by selecting options in the **Sound Effects** group box.


Lists the sounds that Guard Dog can play when it displays a Privacy Alert. Select **Quiet** to turn off the sound. Click the button  to listen to the selected sound. (You must have a sound card and speakers to play a Guard Dog sound.)

Lists the sounds that Guard Dog can play when it displays a Security Alert. Select **Quiet** to turn off the sound. Click the button  to listen to the selected sound. (You must have a sound card and speakers to play a Guard Dog sound.)

Lists the sounds that Guard Dog can play when it displays a Virus Alert. Select **Quiet** to turn off the sound. Click the  button to listen to the selected sound. (You must have a sound card and speakers to play a Guard Dog sound.)

Lists the sounds that Guard Dog can play when it displays a Privacy Alert. Select **Quiet** to turn off the sound. Click the  button to listen to the selected sound. (You must have a sound card and speakers to play a Guard Dog sound.)

Lists the sounds that Guard Dog can play when it displays a Security Alert. Select **Quiet** to turn off the sound. Click the  button to listen to the selected sound. (You must have a sound card and speakers to play a Guard Dog sound.)

Lists the sounds that Guard Dog can play when it displays a Virus Alert. Select **Quiet** to turn off the sound. Click the  button to listen to the selected sound. (You must have a sound card and speakers to play a Guard Dog sound.)

Scheduler Protection Settings

You can schedule when Guard Dog performs actions or displays reminders using the options on the Scheduler Protection Settings page. You can schedule:

- Virus checks.
- Encryption or decryption of File Guardian files.
- Removal of deleted files.
- Reminders to check for the Guard Dog program or virus pattern updates.

Lists the events that you have scheduled. The name of the event appears in the **Name** column and the frequency, date and time of when the event is to run appears in the **When** column. Guard Dog uses the **Next run time** and **Last run time** columns to display information that is useful for events that run more than one time.

Removes the selected scheduled event from the list.

Starts the **Add Scheduled Event** wizard for a selected event, which lets you change settings for the event.

Adds an event to the schedule using the **Add a Scheduled Event** wizard.

Cookie Blocker Protection Settings

The Cookie Blocker Protection Settings page contains options that let you choose whether to accept or reject cookies from the Web sites you visit. Thus, you can enjoy the benefits that cookies offer at your favorite Web site while blocking new cookies from other sites.

You can use the options in the **Sites setting cookies** group box to control how Guard Dog should respond when a Web site sends a cookie to your PC the first time.

A direct site is any location on the Internet that you visit by typing in the address (also known as the Universal Resource Locator) for the site, or visit by clicking a hyperlink that connects one Web site to another. If you connect with a site directly, any cookies sent are likely to be used for your benefit. Reputable sites will tell you if you must accept a cookie in order to view their site.

You can set up Guard Dog to do one of the following when you go directly to a Web site:

- ▶ **Accept**—Guard Dog allows the direct Web site to automatically set cookies on your PC.
- ▶ **Reject**—Guard Dog adds the Web site to **Rejected** list and then blocks the exchange of cookies when you go directly to the site.
- ▶ **Prompt**—Guard Dog displays an alert message when you visit a site directly and asks whether to **Accept Always** or **Never Accept** cookies from this Web site.

Allows cookies to be exchanged between your computer and any Web site that you connect with directly. A direct site is any location on the Internet that you visit simply by typing in the address (also known as the Universal Resource Locator or URL) for the site, or visit by clicking a hyperlink that connects one Web site to another.

Blocks the exchange of cookies between your computer and any Web site that you connect with directly. A direct site is any location on the Internet that you visit simply by typing in the address (also known as the Universal Resource Locator or URL) for the site, or visit by clicking a hyperlink that connects one Web site to another.

Asks whether to block the exchange of cookies each time you visit a Web site that you connect to indirectly. A direct site is any location on the Internet that you visit simply by typing in the address (also known as the Universal Resource Locator or URL) for the site, or visit by clicking a hyperlink that connects one Web site to another.

An indirect Web site is a site that you connect to without your knowledge. Frequently, when you go directly to a commercial Web site, you also connect indirectly with other Web sites that set cookies in order to monitor your browsing habits. For example, a site you are visiting directly may have an advertisement on their page that comes from another Web site. The site that provides the advertisement can set a cookie that helps them track whether you visit other sites that use their ads.

You can set up Guard Dog to do one of the following:

▶ **Accept**—Guard Dog allows the indirect Web site to automatically set cookies on your PC.

▶ **Reject**—Guard Dog adds the Web site to **Rejected** list and then blocks the exchange of cookies between your PC and the indirect Web site.

▶ **Prompt**—Guard Dog displays an alert message when you visit a site indirectly and asks whether to **Accept Always** or **Never Accept** cookies from this Web site.

Allows cookies to be exchanged between your computer and any Web site that you connect with indirectly. An indirect site is any location on the Internet that you connect to *without* typing in the Web address (also known as the Universal Resource Locator or URL) or without clicking a hyperlink for that site. Usually you will connect to an indirect site as a result of connecting to a direct site that displays content coming from the indirect site.

Blocks the exchange of cookies between your computer and any Web site that you connect with indirectly. An indirect site is any location on the Internet that you connect to *without* typing in the Web address (also known as the Universal Resource Locator or URL) or without clicking a hyperlink for that site. Usually you will connect to an indirect site as a result of connecting to a direct site that displays content coming from the indirect site.

Asks whether to block the exchange of cookies each time you visit a Web site that you connect to indirectly. An indirect site is any location on the Internet that you connect to *without* typing in the Web address (also known as the Universal Resource Locator or URL) or without clicking a hyperlink for that site. Usually you will connect to an indirect site as a result of connecting to a direct site that displays content coming from the indirect site.

Displays the Web sites that you have visited and whether you have allowed your computer to exchange or reject cookies from those sites.

As you visit new Web sites, Guard Dog accepts cookies based on the choices you made in the **Sites setting cookies** group box. If you select **Accept**, Guard Dog allows the cookies to be set. If you select **Prompt**, Guard Dog displays its Cookie Blocker alert message. If you respond to the message by clicking **Accept Always**, Guard Dog adds the site name in the **Allowed** list. The Web sites in this list have your permission to exchange cookies with your computer without provoking a Cookie Blocker alert. After Guard Dog adds a site to the **Allowed** list, you can move it to the **Rejected** list using **>>** or delete it from either list using **Remove**.

As you visit Web sites , Guard Dog rejects cookies based on the choices you made in the **Sites setting cookies** group box. If you select **Reject**, Guard Dog prevents cookies from being set. If you select **Prompt**, Guard Dog displays its Cookie Blocker alert message. If you respond to the message by clicking **Never Accept**, Guard Dog adds the site name in the **Rejected** list. The Web sites in this list are those that are not allowed to exchange cookies with your computer. After a site is on the **Rejected** list, you can move it to the **Allowed** list using >> or delete it from either list using **Remove**.

Moves the selected Web site from the **Allowed** list to the **Rejected** list.

Deletes the selected Web site from either list. If you visit this Web site again, Cookie Blocker may ask you about accepting or rejecting cookies based on the options you have selected in the **Sites setting cookies** group box.

Moves the selected Web site from the **Rejected** list to the **Allowed** list.

Identity Protector Protection Settings

The Identity Protector Protection Settings page allows you to specify what personal and financial information to protect. If a program attempts to send out this information over the Internet, Guard Dog warns you based on the options you choose when you add the information.

Guard Dog displays the personal information that you entered either during the Privacy portion of the Interview or directly in Identity Protector. By default, Guard Dog alerts you when this information is about to be sent out over the Internet. You can change the alert options selecting an entry and clicking **Edit**. You can add and delete information from Identity Protector using **Remove** and **Add**.

Displays the personal information that you entered either during the Privacy portion of the Interview or directly in Identity Protector. You can work with this information using the **Remove**, **Edit**, and **Add** buttons.

Removes the selected entry from the list.

Starts the **Add Identity Information** wizard, which displays the existing information for the selected entry. Change the information you want and click **Finish** on the last page of the wizard to save your changes.

Starts the **Add Identity Information** wizard, which steps you through adding personal information to protect.

Guard Dog displays the financial information that you entered during the Privacy portion of the Interview or that you added directly in Identity Protector Protection Settings page. By default, Guard Dog alerts you when this information is about to be sent out over the Internet. You can change the alert options selecting an entry and clicking **Edit**. You can add and delete information from Identity Protector using **Add** and **Remove**.

Displays the financial information that you entered either during the Privacy portion of the Interview or that you entered directly in Identity Protector Protection Settings page. You can work with this information using the **Remove**, **Edit**, and **Add** buttons.

Removes the selected entry from the list.

Starts the **Add Financial Information** wizard, which displays the existing information for the selected entry. Change the information you want and click **Finish** on the last page of the wizard to save your changes.

Starts the **Add Financial Information** wizard, which steps you through adding financial information to protect.

Web Trail Cleaner Protection Settings

The Web Trail Cleaner Protection Settings page allows you to remove the Internet history files and delete files from the browser cache either after you exit your browser or depending on which browser you are using, when you close Windows. Guard Dog gives you complete control over what the Web Trail Cleaner removes.

Select **Prompt to clean up after closing Web browser** if you want to control the deletion of your browsing history and Internet junk files. You will be prompted to clean your files:

- Each time you close your Netscape or Internet Explorer browser.
- When you shut down Windows, if you are using Internet Explorer and any browsing files exist.
- When you shut down Windows, if you are using Microsoft's Active Desktop.

Select **Automatically Clean Up after closing Web browser** if you want Web Trail Cleaner to delete your browsing history and Internet junk files. Web Trail Cleaner does its work:

- Each time you close your Netscape or Internet Explorer browser.
- When you shut down Windows, if you are using Internet Explorer and any browsing files exist.
- When you shut down Windows, if you are using Microsoft Active Desktop.

Select **Keep bookmarked items** so that Web Trail Cleaner will not delete the browsing files associated with sites that you have bookmarked (or have selected as Favorites).

Select the **Keep bookmarked items** check box so that Web Trail Cleaner will not delete the browsing files associated with sites that you have bookmarked (or selected as a Favorite) after you close your browser. Bookmarks allow you to connect quickly to a site without typing in the URL for each Web site that is important to you or that you visit frequently. This option is available only if you selected **Automatically Clean Up after closing Web browser**.

Search Filter Protection Settings

Prevents search-related information from one Web site being sent to the next site you visit. In order to make your Browser's Back button work, the Web site that you are leaving passes on referral information to the next site you are visiting. Part of that referral information can contain search-related information from the previous site. When **Search Filter** is turned on, Guard Dog trims any search-related data before passing on the referral information.

Gatekeeper Protection Settings

The Gatekeeper Protection Settings page allows you to set up Gatekeeper to warn you when certain potentially harmful activities occur so that you can decide how to proceed. Gatekeeper keeps a watchful eye over your computer and what goes on as you use the Internet.

The entries in this box represent actions that your Internet-related programs can perform that could have harmful consequences. Based on how you use the Internet, decide which actions warrant a warning from Gatekeeper and select the associated check box.

Warns you when you start to connect to a site that has been known to contain harmful ActiveX controls or Java programs, viruses, or Trojan Horses.

Warns you when your modem dials without the sound turned on. Some programs can collect sensitive information from your computer and use your modem to send it somewhere else.

Warns you when a program starts to launch another program without your permission. For example, a hostile program may try to launch your Web browser.

Warns you when a program sends out over the Internet any number that resembles a credit card number. Some hostile programs are designed to search for credit card numbers and send them to another site.

Lists the programs to which you have given permission to access the Internet without displaying an alert message. Initially, Guard Dog checks with you each time a program, such as your browser, accesses the Internet. If you answer **Allow Always** to the alert message, Guard Dog adds the program to this list and doesn't warn you again about the program. Review these programs periodically and decide whether to keep them in the list or remove them.

Removes the selected program from the list. The next time the program tries to access the Internet, Guard Dog displays an alert message to ask for your permission.

File Guardian Protection Settings

The File Guardian Protection Settings page allows you to protect sensitive or critical files on your computer by specifying which programs have access to them. For example, you can protect your e-mail files so that only the mail program can use them. Additionally, you can set up File Guardian to warn you when another program, such as an ActiveX control, performs actions that may be harmful to the data in your files.

The entries in this box represent actions that could have harmful consequences to the data on your computer. Based on your security needs and how you use the Internet decide which actions warrant a warning from File Guardian and select the associated check box.


Warns you when an ActiveX control scans files on your PC. ActiveX controls can perform harmless scans, such as when it needs to check which files you have on your PC in order to update files for the Web site using the ActiveX control. However, an ActiveX control can be designed to compromise your security, for instance it may be looking for files containing private financial information to send to another location. Select this check box to receive an alert message.

Warns you when a program begins to format any hard drive—including Jaz and Zip drives. Reformatting your computer's hard drive without your knowledge can have catastrophic results. Not only do you lose valuable data, but you also lose valuable time trying to return your computer to its former functioning state. Select this check box to receive an alert message.

Warns you when an ActiveX control deletes a file on your PC. ActiveX controls can delete files for legitimate reasons; for example, deleting the temporary files it may have created when you downloaded files from the Web site running the ActiveX control. However, an ActiveX control may be designed to delete important files as well. Select this check box to receive an alert message.

Warns you when a program begins to access any Windows password file (.pwl file). Passwords are an important security feature, as they control who has access to shared resources that are available to your PC. Select this check box to receive an alert message.

Displays the list of files that File Guardian monitors and which programs have access to them. You can add to or remove files or programs from the lists.

Displays the list of files that you have selected for File Guardian to monitor. The files are displayed using the method by which you selected them—by filename, folder or drive in which they are stored, file group, or file type. If you select the **Include for encryption** check box on the **Add Guarded File Wizard** dialog box, a lock icon appears by the file. To encrypt (or decrypt the file), click the Guard Dog icon  on the system tray and select **Encrypt File Guardian files** (or **Decrypt File Guardian files**) from the pop-up menu.

Displays the list of programs that you have authorized to access the selected file. File Guardian displays an alert message and asks you for authorization the first time a program tries to access a file in the Guarded list. If you respond to the alert message by clicking **Allow Always**, File Guardian adds the program to the **Programs that have access to this file** list.

Removes the selected file or program from the **Guarded Files** or **Programs that have access to this file** lists.

Starts the Add Guarded File Wizard, which guides you through adding files to the **Guarded Files** list or specifying what programs can have access to the files in this list. Select the file to guard first, before you click the **Add** button to grant file access to a program.

Password Manager Protection Settings

The Password Manager Protection Settings page allows you to store securely Web site passwords. Some Web sites control access by requiring you to enter a user name and password each time you visit the site. When you visit a password-protected site, just open Browser Buddy and drag and drop the login information from Password Manager into the Web site's login form.

Displays the list of records stored by Password Manager. Each record contains the name of the Web site and the username and password that you use to log into the site.

Deletes the selected record from the Password Manager list.

Opens the **Enter password to save** dialog box, which displays the information for the selected record.

Opens the **Enter password to save** dialog box, where you can store the name of the Web site and your username and password for the site.

Virus Sentry Protection Settings

The Virus Sentry Protection Settings page allows you to specify how Guard Dog protects your PC from virus infection. From this page, you can specify as-you-work virus checking options using **When to check**, as well as specify what types of files Virus Check (in CheckUp) scans using **What to check**.

Use the as-you-work options in this box to control what actions Virus Sentry monitors as you work on your PC.

Use this as-you-work option to scan any program for viruses when it starts up.

Use this as-you-work option to scan any e-mail attachment for viruses when it is opened.

Use this as-you-work option to scan any file for viruses when it is opened.

Use this as-you-work option to scan any file for viruses when it is moved or renamed.

Use this as-you-work option to scan any floppy disk for viruses when it is accessed.

Scans DOS for viruses and identifies them before Windows loads. The Windows operating system still depends on functions provided in an older disk operating system called DOS. Some viruses such as boot sector viruses, partition table viruses, and memory viruses can infect files before Windows loads. Although these virus types may be detected in Windows, most must be cleaned in DOS. For this reason, you should select this setting for more complete virus protection.

Determines how Guard Dog responds when it finds a virus in the program types or document files you specified in **What to check**.

You can control the action that Virus Sentry takes when it finds a virus in the program types or document files you specified in **What to check**. You can tell Virus Sentry to:

- **Prompt**—You can decide what to do on a case-by-case basis.
- **Deny access**—Blocks you from doing anything with the file, except for deleting it with Windows Explorer or cleaning it with CheckUp. (When an infected file is opened, the virus spreads.)
- **Automatic delete**—Deletes the file from your hard drive.
- **Automatic clean**—Removes the virus from the infected file, or failing that, Guard Dog will prompt you to delete the file.
- **Shut down computer**—Shuts down Windows without taking additional action.

Determines what types of files Guard Dog scans during a CheckUp.

Determines which type of files Guard Dog scans during a CheckUp. You can tell Guard Dog to scan:

- **All Files**—Checks every file on your computer. This is the most complete check, but also the most time-consuming check if you have a lot of files on your computer. It will catch viruses in files that use non-standard file types.
- **Program Files**—Checks all files that a program requires in order to run. It checks files using the most common program file extensions, such as .com, .exe, .bat, .bin, .ovl, .drv, .dll, .sys, .tsk, .vxd, and .ocx. This setting will not catch macro viruses.
- **Document Files**—Checks only data files that can contain viruses, which are typically macro viruses. For example, Microsoft Word and Excel document files, and file compression documents such as .zip, .arc, and .lzh. This setting will not catch program viruses.
- **Program Files and Document Files**—Checks both program and document files. This setting will find most viruses and is less time-consuming than checking all files.

Tip

Use **Edit** to add, remove or customize the types of files that are checked during CheckUp.

Customizes the types of document files or program files that Guard Dog checks during CheckUp. On the **Program Files** tab or **Document Files** tab, use the **Add** and **Remove** buttons to specify the types of files and programs to check for viruses.

You can specify the types of files Guard Dog checks during a CheckUp by adding them to the **Program Files** or **Document Files** tab.

Displays the list of program files that Virus Sentry checks during a CheckUp.

Displays the list of document files that Virus Sentry checks during a CheckUp.

Adds file types to the selected **Program Files** or **Document Files** list.

Removes file types from the selected **Program Files** or **Document Files** list.

Controls which files and folders Virus Sentry does not check during any type of virus scan, except for the as-you-work options in the Virus Sentry **When to check** box.

Displays the files and folders that Virus Sentry does not check during any type of virus scan, except for the as-you-work options in the Virus Sentry **When to check** box.

Use the **Add Files** button to include files in the **Do not check...** list.

Use the **Add Folders** button to include folders in the **Do not check...** list.

Use the **Remove** button to delete selected files or folders from the **Do not check...** list.

Tip

Use SHIFT+CLICK to make multiple selections in this list.

Scans DOS for viruses and identifies them before Windows loads. The Windows operating system still depends on functions provided in an older disk operating system called DOS. Some viruses such as boot sector viruses, partition table viruses, and memory viruses can infect files before Windows loads. Although these virus types may be detected in Windows, most must be cleaned in DOS. For this reason, you should select this setting for more complete virus protection.

Interview - Welcome to Guard Dog!

Guard Dog needs some information about you so that it can take up its post as sentry and guard your privacy as you use your PC. After you enter personal information on the next few screens, you can rest assured that this information will travel no farther than an encrypted file on your hard drive. Guard Dog will not divulge anything that it knows about you to anyone else and ensures that no other program can use the information that it has stored.

You can use the **Next** and **Back** buttons to navigate through the Interview. If you want to change or add to your original entries, click **Options** on the Guard Dog Home screen and select **Interview** from the drop-down menu.

Interview - Privacy

Guard Dog offers a variety of protection features designed to guard your privacy especially as you the Internet. The settings on the next few screens are designed to warn you when something happens that could jeopardize your privacy.

Interview - Identity Protector Personal Information

Guard Dog keeps an eye on the information that you enter on this screen and warns you when a person or program tries to send out anything that you have entered here over the Internet. When you run the Guard Dog CheckUp, it also uses the Identity Protector information to identify any files that contain this information and allows you to protect these files with File Guardian.

Use the TAB key to move from box to box and click **Next** to continue to the next Interview screen.

See the following topic, if you want to add, remove, or change anything after completing the Interview.

[About Identity Protector](#)

Interview - Identity Protector Financial Information

If you have financial information on your PC—for instance, you may use a bookkeeping program to balance your check book and pay your bills electronically—Guard Dog can protect this information from other programs that may try to retrieve it and send it to another computer.

Click in a box to position the cursor and start typing.

See the following topic If you want to add, remove, or change anything after completing the Interview.

[About Identity Protector](#)

Interview - Guard Dog Password

Guard Dog wants to maintain security even in its own backyard. You are encouraged to assign a password to the Guard Dog program so that only you can access **Protection Settings**.

If others share your PC, you can use the password to protect your personal and financial information. If the Guard Dog password isn't entered after Windows starts, Guard Dog blocks any information that is protected by Identity Protector from being sent out over the Internet.

If you do not select a password during the Interview, you can assign one later. You can either run the Interview again or change the setting directly from the **Preferences** page.

See the following topics if you want more information about restarting the Interview to change settings or changing the password directly on the Preferences Protection Settings pages.

[Responding to Interview questions](#)

[About Guard Dog Preferences](#)

Interview - AntiVirus

A virus at the very least can be a nuisance and at its worst can destroy valuable data on your PC. Set your mind at ease by letting Guard Dog check for viruses. After the Interview, you can determine exactly which types of files the AntiVirus program checks.

Select the following check boxes to check for viruses

- **Whenever Windows starts up**—Guard Dog automatically checks high-risk files (document files and program files) when Windows starts.
- **Automatically whenever there is some file activity or download**—Guard checks for virus upon:
 - Program execution
 - Email file access
 - File open
 - Move or Rename
 - Floppy drive read

See the following topics for more information about setting up virus protection.

[Getting the most out of AntiVirus protection](#)

[About Virus Sentry](#)

Interview - Emergency Disk

An Emergency Disk is a good backup to have in case something happens to the data that Guard Dog is protecting. The disk contains a copy of this information as well as a program that allows you to start your PC in DOS mode. If you do not make an Emergency Disk, you can set up Guard Dog to remind you to do it later.

See the following topic for information about setting up schedules and the types of events that can be scheduled.


[About the Scheduler](#)

Interview - Summary

You can verify the information that you have given Guard Dog at a glance. If you need to make changes, just click the **Back** arrow until you get to the right screen.

Interview- You are done!

Congratulations! You've given Guard Dog the information that it needs to guard your privacy and keep the sensitive data on your PC secure. When you click **Finish**, Guard Dog will write this information (called settings) to your hard drive then restart your PC.

As an indication that Guard Dog is on duty, an icon  appears in the taskbar at the bottom of your PC's screen. Right-click this icon to display a pop-up menu and choose **Exit** to remove Guard Dog from memory.

Remember that after you do this, Guard Dog can no longer monitor your PC and protect your data from unwarranted intrusion. To start Guard Dog again, double-click the desktop icon.



CyberMedia
Guard Dog

See the following topic for information about the selections on the pop-up menu.

[About the pop-up menu](#)

About Privacy

Each day more and more people visit the World Wide Web just to look around (or, to use the popular term, browse), share information with others, download data, and even buy things. Internet Service Providers offer e-mail services that make communications with others around the world as easy as typing a message and pressing a button to send it to its destination. Clearly, we can benefit from advanced communication opportunities, and the Internet has a nearly limitless opportunity to flourish. However, with these benefits come certain drawbacks.

The advances in communications and data transmission enable others on the Internet to capture, store, and reuse a tremendous amount of personal information. Information can accompany you as you use the World Wide Web. This happens frequently as you browse. For example, if you search for something using one of the readily available Internet search engines, your search requests go not only to the search engine but also to several other sites including the site which provides the advertising banners that you see on many Web sites. Other information also passes as you browse from site to site.

This inter-site information is recorded and correlated with cookies allowing certain Web sites to build databases about you and your interests. Guard Dog's Search Filter blocks the passing of this information.

We agree that a certain amount of privacy is essential to maintain control over our lives and that this privacy must be safeguarded. While we agree that we should, we are just beginning to explore how to guard our privacy in the World Wide Web. CyberMedia offers Guard Dog as a comprehensive solution to the privacy and security issues that you may encounter as you venture into the world of the Internet.

[Read more about security](#)

CyberMedia Privacy Policy

In keeping with our commitment to safeguard the computer user's security and privacy, we would like to assure you that it is not CyberMedia's practice to gather usage information for its own purposes; nor do we collect personal information, such as your name and address, for resale or distribution to other companies to use to create mailing lists or to use in promotional advertising schemes.

This policy applies in full to Guard Dog. The intent behind the design of Identity Protector is to give you complete control over who receives your personal information. This means that Guard Dog will not communicate the personal and financial information entered in Identity Protector to any outside source without your express permission.

About security

With the explosion of interest in the Internet and the expansion of the World Wide Web to offer goods and services in exchange for money, security is becoming an important issue. Business transactions must be protected on both sides—the buyer and the seller. The problem with conducting business over the Internet is easy to define. While it is relatively easy to set up a Web site to display and sell things, it is not so easy to develop mechanisms to ensure the security of the information that must be passed back and forth to accomplish any type of transaction. Moreover, there are people (called hackers) who have the skills, the software, and the inclination to monitor transactions and snare important data like credit card and bank account numbers.

However, there is hope. An encryption technology called “Secure Sockets Layer” has been incorporated into Microsoft Internet Explorer and Netscape browser software. When you choose to use this technology, an icon appears in the browser to indicate SSL is active; and when you do use it, you can be fairly certain that your transaction is safe.

Encryption is great, but again, we are faced with a couple of problems. First, not all servers and browsers are SSL-enabled. SSL software adds to the investment cost associated with the server and can slow server transactions. Second, Microsoft and Netscape did not coordinate their security efforts meaning that although neither company’s browser is immune to security problems, they are not necessarily the same ones. You could very easily be at a loss to assess your security risk and have to rely on flipping a coin to determine which browser is the safer. However, the companies are attuned the risks and pitfalls involved in implementing security measures and are working to correct their problems.

Secure transactions are only part of the problem. Once Web servers receive information, they must be able to keep it safe. In a large network, one in which a Web server is just one of several types of server, the network administrator tries to isolate the Web servers from other mission-critical servers. However, some Web programs interact with data stored on other servers, thus opening a door to potentially sensitive data. Hackers target Web servers because the technology to secure these servers is still developing. A security technology called a “firewall” can control unauthorized access to sensitive data, but must be properly maintained. Even in the most well kept systems, a firewall cannot protect certain services.

From the user’s perspective, there are one or two ways to tell if you can safely transmit information to a Web Site.

First, most business-oriented Web sites do implement server security and will notify you that you are using a secure connection. If the site is not secure, you are warned that you are sending information to a non-secure site and are given the option to continue. Second, most browsers are intelligent enough to detect the security level of the site you are connected to and will display this information.

It is always wise to use every security measure available to you because the world is filled with dishonest people who will take advantage of the unprotected. Microsoft and Netscape are working diligently in the security field to develop advanced solutions and to remedy security leaks in existing Internet products. To take advantage of their latest developments, keep your browser software up-to-date by running Guard Dog frequently.

About viruses

As you use e-mail or browse Web sites , each session carries with it the risk of infecting the data on your PC with a virus.

A virus is a program intentionally designed to affect your PC by attaching itself to a good program. While you use the program, the virus actively copies itself to other programs, thus infecting your PC like a virus infects the body. Most virus programs are just nuisances that take up disk space and cause programs to behave in unexpected ways. However, some virus programs, for example boot sector and partition table viruses, can attack and seriously damage the files that your PC needs to start and load the operating system.

CyberMedia works constantly to identify viruses and places the information about known viruses and their cures in a virus pattern file. As new viruses are identified, the pattern file is updated.

Protecting that data means using a good virus detection program like the one that can be found in Guard Dog. You can help Guard Dog efficiently detect a clean viruses by using Guard Dog to retrieve the latest version of the virus pattern file.

Interview- Cookie Blocker

Generally speaking, cookies can help a Web site better serve you by using information it has previously obtained and stored on your PC. For example, cookies can allow your favorite merchandising site to display custom information for you each time you visit. A password-protected Web site may use a cookie to store your password information so that you don't have to enter it each time you visit the site. Also, some sites require cookies in order to work correctly. These sites will usually warn you that you must accept a cookie.

Cookies can also represent a threat to your privacy because you don't know what is being tracked or who is collecting information about you. Cookie Blocker lets you control who can send cookies to your PC. Thus, you can enjoy the benefits that cookies offer at your favorite Web site while blocking new cookies from other sites.

Cookies from Web sites I visit are cookies that come from Web sites that you visit directly by typing the Web address in your browser or by clicking a link in a Web page. Choose one of the following:

Accepted Always to automatically accept cookies from sites that you connect to directly.

Rejected Always to automatically refuse cookies from sites that you connect to directly..

Prompt for Action to choose whether to accept or reject a cookie from a direct site on a case-by-case basis. As you browse the Web, Guard Dog asks you each time a direct site tries to send a cookie to your PC then adds the site to either the

Accepted or Rejected lists on the Cookie Blocker Protection Settings page.

Cookies from other sites are cookies that come from Web sites that you connect to indirectly—without typing the Web address in your browser or by clicking a link in a Web page. Typically, you connect to these sites because their content is displayed as part of a Web page that you did choose to visit. Choose one of the following:

Accepted Always to automatically accept cookies from sites that you connect to indirectly.

Rejected Always to automatically refuse cookies from sites that you connect to indirectly.

Prompt for Action to choose whether to accept or reject a cookie from an indirect site on a case-by-case basis. As you browse the Web, Guard Dog asks you each time an indirect site tries to send a cookie to your PC then adds the site to either the Accepted or Rejected lists on the Cookie Blocker Protection Settings page.

See the following topic for more information about changing Cookie Blocker settings after you have completed the Interview.

[About Cookie Blocker](#)

Interview - Web Trail Cleaner

As you cruise the Internet, your browser stores files that make it faster to display and return to pages that you've already visited. However, these files can be viewed by others that have access to your PC—either directly or through the Internet. Web Trail Cleaner helps you maintain privacy and security by removing the Internet history files and deleting files from the browser cache. An added benefit to removing the Internet junk files that collect on your PC's hard drive is that it frees up disk space.

Automatically clean up deletes the files when you close your browser or depending on which browser you are using, when you close Windows.

Prompt to clean up asks you to select the sites for which you want to delete browser trail information.

No Action turns off Web Trail Cleaner.

See the following topic for more information about changing Web Trail Cleaner settings after you have completed the Interview.

[About Web Trail Cleaner](#)

Interview- Security

Guard Dog offers several security features that are designed to protect the data on your PC from harm from the outside world. It is always wise to use every security measure available to you because the world is filled with dishonest people who will take advantage of the unprotected.

Interview - Search Filter

As you browse the Internet, information about what you search for at one Web site can be passed on to the next site to which you connect. For instance, you perform a search for "cybermedia" using a popular search engine at your Internet service provider (ISP) site. After you click Search, the address that appears in your browser is

<http://www-isp.net/cgi-bin/query?pg=q&dp=val&who=isp&what=web&kl=XX&q=cybermedia&search.x=38&search.y=10>

The next site that you visit can look at that information to see where you came from and what you searched for. Search Filter will remove all information after the referring Web site address before you connect to the next site.

Yes, Enable Search Filter—Turns on Search Filter in Protection Settings.

No, Disable Search Filter—Turns off Search Filter in Protection Settings.

See the following topic for more information about turning the Search Filter off and on after you have completed the Interview.

[About Search Filter](#)

Interview - Gatekeeper

The Gatekeeper keeps a watchful eye over your PC and what goes on as you use the Internet. Gatekeeper acts as your safety net warning you when you are about to connect to a Web sites that contains harmful content such as ActiveX controls or Java applets. Other programs that you install on your PC can come from many sources, some of which may or may not be entirely reliable. You really can't tell what a program is going to do until you install and use it. Something that is seemingly innocent may be designed to look for certain types of information on your PC and use the Internet to transmit this information to another computer.

You can select the Gatekeeper options on this Interview screen to warn you when certain potentially harmful activities occur so that you can decide how to proceed.

When an unauthorized program tries to access the Internet—Warns you when a program tries to access the Internet.

When going to Web sites know to contain hostile ActiveX and viruses— Warns you when you start to connect to a site that has been known to contain harmful ActiveX controls, viruses, or Trojan Horses.

If my modem dials out silently— Warns you when your modem dials without the sound turned on. Some programs can collect sensitive information from your PC and use your modem to send it somewhere else.

If any Credit Card number is sent out over the Internet— Warns you when a program sends out over the Internet any number that resembles a credit card number. Some hostile programs are designed to search for credit card numbers and send them to another site.

See the following topic for more information about changing Gatekeeper settings after you have completed the Interview.

[About Gatekeeper](#)

Interview - File Guardian

File Guardian protects sensitive or critical files on your PC. File Guardian can automatically protect your files so that only the programs that you specify can use them by adding them to the Guarded Files list. For added protection, you can encrypt files protected by File Guardian. The encrypted files are unusable until you decrypt them. You can select the following types of files to protect:

Password files

Guard Dog warns you when a program begins to access any Windows password file (.pwl file). Passwords are an important security feature, as they control who has access to shared resources that are available to your PC. Guard Dog monitors them when you select this check box.

E-mail files

File Guardian allows you to quickly protect sensitive files associated with most types of e-mail programs by adding these files to Guarded Files list as a group.

The E-mail file group includes files for:

- Internet Explorer 4 E-mail
- Internet Explorer 3 E-mail
- Internet Explorer 4 Outlook Express E-mail
- Netscape E-mail
- Communicator E-mail
- Eudora E-mail
- AOL 3 Mail and Password Files

Financial files

Guard Dog also recognizes the files associated with these financial programs and adds them as a group to the Guarded Files list.

The Financial file group includes files for:

- Microsoft Money Financial
- Quicken Financial

Note

If you choose not to guard e-mail or financial files here or if you install any of the above listed e-mail or financial programs later, you can protect them by adding their file groups to the Guarded Files list in File Guardian Protection Settings.

See the following topic for more information about adding, removing, or changing the information protected by File Guardian.

[About File Guardian](#)

Interview - Password Manager

Can you remember the password and user name for every protected site that you visit? If you have committed them to paper, do you remember where you put the list and do you have a safe place to keep it? If you let Guard Dog manage your passwords, you won't have to worry about the answers to these questions.

Instead of typing your user name and password each time you visit a password-controlled Web site, Password Manager allows you to drag and drop this information from Browser Buddy to the appropriate boxes on login screen.

Site—This name is only displayed in the list. You can enter either the site's address or its name.

Username—This is the name by which you identify yourself to the Web site. It is also known as a login name, user ID, member name, and so on.

Password—This is the password with which you verify your identity to the Web site. For your protection, each character appears as an asterisk in Guard Dog.

See the following topic for more information about adding passwords and usernames to Password Manager after you have completed the Interview.

[About Password Manager](#)

Browser Buddy is a convenient way to get a summary of cookie activity. You can choose:

- **All Web Sites**—Choose this to receive the total number of cookies exchanged between your PC and all the Web sites that you have visited since you last cleaned cookies from your computer
- **Local Sites**—Choose this to receive the total number of cookies exchanged between your PC and the site that you are connected to currently.

Browser Buddy provides access to the passwords and usernames that you enter in Password Manager. To access a password, click the arrow by the Password Manager drop-down list and select the Web site that you are connecting to from the list. The password and user name for your selection is displayed in the Password Manager box at the bottom of Browser Buddy. To add a new password to Password Manager, click the arrow and choose **Add New Entry**. Type in the information in the Enter password to save dialog box and click **OK**.

Displays the total number of cookies sent to your computer based on the selection you made in Statistics.

Displays the total number of cookies rejected based on the selection you made in Statistics.

Displays the total number of times Guard Dog stopped your information from being sent to an indirect Web site.

Drag and drop your username and password from Browser Buddy to the appropriate boxes on the login screen each time you visit a password-controlled Web site.

Guard Dog Home screen

The Guard Dog Home screen is your entry point to the Guard Dog program. Your choices are:

{button ,PI('gd.hlp','CheckUp_button_on_the_main_GD_window')} CheckUp

{button ,PI('gd.hlp','Update_button_on_GD_main_window')} Update

{button ,PI('gd.hlp','Log_button_on_the_main_GD_window')} Log

{button ,PI('gd.hlp','Options_button_on_the_main_GD_window')} Options

{button ,PI('gd.hlp','Help_button_on_the_main_GD_window')} Help

Click **Options** on the Guard Dog Home screen and click **CheckUp Settings** in the drop-down menu to change what Guard Dog checks during CheckUp. CheckUp scans your PC to identify issues related to privacy, security, and virus protection. If CheckUp finds something that needs your attention, these items are displayed in the CheckUp Found screen.

Click **Update** to get the latest improvements to the Guard Dog program, as well as the latest virus pattern files. CyberMedia places new virus pattern files on its Web site monthly. Guard Dog uses CyberMedia's Oil Change technology and your Internet connection to check for and retrieve the latest improvements from CyberMedia.

Click **Log** if you want to know what Guard Dog has been doing. From the Log screen, you can print or clear the log.

Guard Dog generates an itemized list of the actions that it has taken. By default, Guard Dog adds information to the list chronologically-meaning that older actions appear at the top of the list while more recent events are added at the bottom. To sort the **Guard Dog Actions** or **Type** lists alphabetically, click their respective column headings. To return to the date format, click **Date/Time**.

Select from the following Options:

Customize CheckUp–Takes you to the Customize CheckUp screen where you can specify what Guard Dog checks for when you run a CheckUp.

Protection Settings–Takes you to the Protection Settings dialog box, which contains Protection Settings pages for all the Guard Dog features. You can specify how Guard Dog behaves when it detects issues that affect the privacy, security and virus protection of your PC.

Interview–Takes you through the Interview where you can specify in a guided manner, how Guard Dog should behave when it detects issues that affect the privacy and security and privacy of your PC.

Click Help to get more information about how Guard Dog works. The Help system provides information about the features and functions available on the screen that you are looking at. The selections available on the Help menu include:

- **Help Topics**—Gives you access to the complete Guard Dog Help system including the Contents, Index, and Find. Click a book in the Contents to display the titles of the topics beneath the book. Click a topic title to display the help topic associated with the title.

The Help system uses standard Windows Help navigation buttons, including **Help Topics** to return from a topic to the table of contents, **Back** to return to the topic you just reviewed, **>>** and **<<** to browse forward and backward through all the topics in the Help system.

- **Help on this screen**—Gives you access to a help topic containing information that has been tailored specifically for the screen that you are viewing. Press **ESC** on your keyboard to close the topic.
- **How Guard Dog works**—Gives you access to the Guard Dog video, which introduces you to Guard Dog and its features.
- **CyberMedia on the Web**—Opens your browser and connects to the CyberMedia Web site where you can get the latest information for all CyberMedia products.
- **Guard Dog on the Web**—Opens your browser and connects to the Guard Dog Home screen on the CyberMedia Web site where you can get the latest Guard Dog information.
- **FAQs**—Opens your browser and give you access to the Frequently Asked Questions page on the CyberMedia Web site.
- **Report a problem**—Opens your browser and displays an e-mail form in which you can describe your problem. Be sure to include as much detail as possible. Your e-mail message will be sent to CyberMedia Support.
- **Virus Encyclopedia**—Gives you access to a Help file that contains detailed information about each virus that CyberMedia has identified. Click the Index tab and select the name of your virus from the alphabetical list.
- **About Guard Dog**—Opens your browser and displays a page containing version and copyright information.

Guard Dog Log

Click Log to see what Guard Dog has been doing to protect the data on your PC. Guard Dog keeps track of what it does on your PC and displays this information in a list format. On the Log screen, you can view the following information:

{button ,PI('gd.hlp','Date_Time_column_on_the_Report_page')} Date/Time

{button ,PI('gd.hlp','Guard_Dog_Action_column_on_the_Report_page')} Guard Dog Action

{button ,PI('gd.hlp','Type_column_on_the_Report_page')} Type

{button ,PI('gd.hlp','User_column_on_the_Report_page')} User

You can decide what to do with the data in the Log. You can:

{button ,PI('gd.hlp','Print_button_on_the_Report_page')} Print

{button ,PI('gd.hlp','Cancel_button_on_the_Report_page')} Cancel

{button ,PI('gd.hlp','Clear_button_on_the_Report_page')} Clear

Look in the Date/Time column to see when Guard Dog performed certain actions.

Look in the Guard Dog Action column to see what Guard Dog did to protect the data on your PC.

Look in the Type column to see which Guard Dog feature took action.

Look in the User column to see which user Guard Dog protected when it took action.

Closes the Log screen and returns to the Guard Dog Home screen.

Sends the information in the Log screen to your printer.

Deletes all the information in the **Log** screen.

Customize CheckUp

You can specify what Guard Dog checks as it monitors the security and privacy of the data on your PC. After you have made your selections, click **Apply** to have Guard Dog save your selections and use them the next time you run a CheckUp. Clicking **Cancel** closes the Customize CheckUp screen without saving any changes you may have made to the items in the CheckUp list.

- **Emergency Disk Check**–Verifies that you've created an Emergency Disk and sets up a reminder in Scheduler to update your disk based on the frequency that you specify.
- **Guard Dog Updates Check**–Runs Update and sets up a reminder in Scheduler to check for updates to Guard Dog based on the frequency that you specify. CyberMedia places updates, including new virus pattern files, on its Web site. Guard Dog uses CyberMedia's Oil Change technology to check for and download available updates.
- **Browser Version Check**–Verifies that your Internet Explorer or Netscape Navigator browser is up-to-date and, if necessary, opens your browser to the Web page that contains an update to your browser.
- **Identity Protection Check**–Finds files on your PC that contain any sensitive information that you added to Identity Protector and allows you to add these files to File Guardian's Guarded File list.
- **Cookie Check**–Determines if cookies have been left behind on your PC and offers to remove them.
- **Search Filter Check**–Determines if files that you have cleaned out of the Recycle Bin still remain on your disk. If Guard Dog finds anything, it will give you the option to delete the data permanently from your hard drive.
- **Web Trail Check**–Determines whether your Web browser has left any Web files or ActiveX controls behind on your PC and offers to remove them.
- **Gatekeeper Check**–Determines which programs on your PC have unrestricted Internet access and allows you to change their access rights. If you are using Internet Explorer, it will check your browser security level.
- **File Guardian Check**–Looks for Outlook, Netscape, Eudora and other e-mail files and Quicken and MS Money financial files, displays whether they are protected by File Guardian, and allows you to protect them.
- **Password Check**–Determines if there are shared folders on your PC that aren't password protected and allows you to add passwords.
- **Virus check**–Lets you select the drives, files and folders that Guard Dog scans for viruses.

Guard Dog Report CheckUp Found

Guard Dog compiles a list of the problems and issues that it finds during a CheckUp. These problems appear under the Security, Privacy and AntiVirus headings on the CheckUp Found screen. When you select a problem, you can perform the following actions:

{button ,PI('gd.hlp','Fix_button_on_the_CheckUp_found_page')} Fix

{button ,PI('gd.hlp','Close_button_on_the_CheckUp_found_page')} Close

Tell Guard Dog what action to take to solve a problem by clicking **Fix**. Guard Dog displays a screen containing important information about solving the problem.

Click **Close** to close this screen and return to the Guard Dog Home screen after you are finished choosing problems. If you left problems unresolved, you can run CheckUp again. These problems and any new ones that Guard Dog may identify will be displayed in the CheckUp Found screen.

CheckUp Found - Deleted Files

When you “delete” files and folders from your PC, they don’t really disappear. The information stays on your hard drive, it is just written over as the space is needed. Guard Dog can detect the data remaining on your hard drive and gives you the option to remove it completely.

{button ,PI('gd.hlp',`Delete_button_the_ChkUp_found_Delete_page`)} [Remove](#)

{button ,PI('gd.hlp',`Cancel_Button_on_the_Complete_Delete_page`)} [Cancel](#)

Click **Remove** to ensure that the files and folders that you delete are completely removed from your PC's hard drive.

Click **Cancel** if you don't want to delete the files that Guard Dog has identified. It returns you to the CheckUp Found screen.

CheckUp Found - Emergency Disk

When disaster strikes the data on your PC, you can recover using the Emergency Disk. The disk contains the important data that Guard Dog was protecting, as well as an emergency program that allows you to start your PC in DOS. You can do the following:

{button ,PI('gd.hlp',`Create_button_on_the_Emergency_Disk_page')} Create

{button ,PI('gd.hlp',`Cancel_button_the_Create_an_Emergency_disk_page')} Cancel

Click **Create** to have Guard Dog save the important, protected data to floppy disks. You will need three 3.5" floppy disks for Guard Dog to use.

Click **Cancel** to return to the CheckUp Found screen if you do not want Guard Dog to create an Emergency Disk. However, it is a good idea to make one as a safeguard against disaster.

CheckUp Found - Emergency Disk Update

The information on your Guard Dog Emergency Disk may be out of date. Have the disks on hand and let Guard Dog update the information for you.

{button ,PI('gd.hlp',`CheckUp_Found_Emergency_Disk_out_of_date_Update_button`)} Update

{button ,PI('gd.hlp',`CheckUp_Found_Emergency_disk_out_of_date_Cancel_button`)} Cancel

Click **Update** to refresh the data on your Emergency Disks.

Click **Cancel** if you don't want to Guard Dog to update the information on your Emergency Disks.

CheckUp Found - Internet Security Level

The Microsoft Internet Explorer browser has security features that protect you as you browse the Internet. Guard Dog checks and warns you when the level is not set to the highest possible setting. You use **Update** to access Internet Explorer and the Safety Level dialog box where you can select:

- High—protects you from all harmful content.
- Medium—warns you of potentially harmful content and lets you decide whether to continue.

Tip

When you choose the highest security setting, Internet Explorer blocks all programs such as ActiveX and Java applets from being downloaded to your PC.

{button ,PI('gd.hlp',`Update_button_on_CheckUp_Found_Internet_Security_Level')} [Update](#)

{button ,PI('gd.hlp',`Cancel_button_on_CheckUp_Found_Internet_Security_Level_page')} [Cancel](#)

Click **Update** to start Internet Explorer and display the Safety Level dialog box.

Click **Cancel** to have Guard Dog leave the settings as they are and return to the CheckUp Found screen.

CheckUp Found - Guard Dog Update

Guard Dog uses CyberMedia's Oil Change technology to check for information about updates for your Internet browser software.

{button ,PI('gd.hlp','Update_available_for_browser_button')} Update

{button ,PI('gd.hlp','Cancel_button_for_second_update_available_for_browser')} Cancel

Click **Update** to start Oil Change to check and retrieve the latest fixes and software improvements.

Click **Cancel** to close this screen and return to the CheckUp Found screen if you don't want to check for Updates.

CheckUp Found - Browser Update Available

Guard Dog uses CyberMedia's Oil Change technology to check for information about updates for your browser software.

{button ,PI('gd.hlp','Update_button_on_second_update_for_browser')} Update

{button ,PI('gd.hlp','Cancel_button_for_second_update_available_for_browser')} Cancel

Click **Update** to check and retrieve the latest fixes and software improvements for your browser.

Click **Cancel** to close this screen and return to the CheckUp Found screen. if you don't want to check for updates for your browser.

CheckUp Found - Guard Dog Update Available

CyberMedia places product improvements and enhancements on its Web Site. Guard Dog uses CyberMedia's Oil Change technology to check the site for the latest improvements to the Guard Dog software including new virus pattern files.

Click **Update** to start Oil Change to check for the latest fixes and improvements to the Guard Dog program.

Click **Cancel** to close this screen and return to the CheckUp Found screen if you don't want to check for updates.

CheckUp Found - Private and Financial files

Guard Dog checks all the files on your hard drive to see if they contain any of the information that you entered in Identity Protector and lists the results in this screen. Guard Dog also determines whether any of these files are being protected by File Guardian and selects them automatically. You can perform the following actions:

{button ,PI('gd.hlp','Protect_button_on_the_CheckUp_protect_page')} Protect

{button ,PI('gd.hlp','Cancel_button_on_the_Protect_file_page')} Cancel

Select the check box by the file name and click **Protect** to add any of the files in this list to the files that are protected by File Guardian.

Click **Cancel** if you don't want to add files to File Guardian. Guard Dog returns to the CheckUp Found screen without making any changes.

CheckUp Found - Remove ActiveX controls

Guard Dog checks your PC for ActiveX controls and displays them in this list. Guard Dog considers controls that have been signed by their creators to be safe and places a check only by unsigned controls. Even if you have downloaded ActiveX controls from a site that you consider safe, you may want to delete them anyway because other Web sites can identify these controls and use them. (If you delete the controls, the next time that you visit the site that sent you the controls, you will have to download them again.) You can perform the following perform the following actions:

{button ,PI('gd.hlp','Remove_button_on_the_CheckUp_ActiveX_control_page')} Remove

{button ,PI('gd.hlp','Cancel_button_on_the_CheckUp_ActiveX_control_page')} Cancel

Select the control and click **Remove** to delete an ActiveX control from your hard drive.

Click **Cancel** to close the screen and return to the CheckUp Found if you do not wish to do anything. Guard Dog does not save any changes that you may have made while the screen was open.

CheckUp Found - Cookies

Guard Dog checks the number of cookies that have been stored on your PC and selects the check box by the cookies that were sent by Web sites that you have bookmarked. Guard Dog does not delete cookies from bookmarked or favorite sites because Guard Dog assumes that the information in the cookie may be needed by your favorite sites. You can perform these actions:

{button ,PI('gd.hlp',`Remove_button_on_the_CheckUp_Cookie_page`)} Remove

{button ,PI('gd.hlp',`Cancel_button_on_the_CheckUp_Cookie_page`)} Cancel

Select the sites whose cookies you want to delete and click **Remove**.

Click **Cancel** if you do not want to take any action in this screen. Guard Dog closes the screen and returns to the CheckUp Found screen.

CheckUp Found - Web Trail files

Web sites routinely download files to your PC, for example images files to allow pages to download faster. These files are junk files that take up space on your hard drive and can be used to track you Web browsing habits.

You can perform the following actions:

{button ,PI('gd.hlp',`Remove_button_on_the_Internet_files_CheckUp_page')}} [Remove](#)

{button ,PI('gd.hlp',`Cancel_button_on_the_CheckUp_Internet_files_page')}} [Cancel](#)

Use **Remove** to get rid of files that are taking up space on your PC's hard drive. Guard Dog will only remove files from sites that you haven't bookmarked or designated as a favorite site. You can select or clear the check boxes by the cookie names to select cookies for Guard Dog to remove.

Click **Cancel** to return to the CheckUp Found screen if you do not want to take any action on this screen.

CheckUp Found - Programs with Internet access

Guard Dog monitors the programs that have access to the Internet and lists them and their locations on your PC's hard drive in this screen. Please review the programs to which you have given Internet access privileges. You can perform these actions:

{button ,PI('gd.hlp',`Deny_Access__button_for_Checkup_Internet_access_page')} Deny Access

{button ,PI('gd.hlp',`Cancel_button_on_the_CheckUp_Internet_access_page')} Cancel

Select a program from the list and click **Deny Access** to remove automatic access to the Internet.

Click **Cancel** to return to the CheckUp Found screen if you do not wish to make any changes.

CheckUp Found - Non-password protected Shared files

Sometimes in network environments it is useful to allow information in specific files to be accessed by other computer users. If your PC is using the Windows operating system, you can easily mark folders as "shared" so that others can have access to them. If you are sharing folders, you should password-protect them so that only those that you give the password to can have access to the information.

{button ,PI('gd.hlp','CheckUp-Shared_files_are_password_protected_Set_Pass_Button')} [Set Password](#)

{button ,PI('gd.hlp','CheckUp-Shared_files_password_protected_Cancel_button')} [Cancel](#)

Select the file, folder, or drive name and click **Set Password** if you want to add password-protection.

Click **Cancel** if you don't want to add password protection to shared files. Guard Dog returns to the CheckUp Found screen without making any changes.

CheckUp Found - Viruses

Guard Dog's Virus Sentry has detected virus infected files. The name and location of each file is displayed in the list at the bottom of the screen. To rid the files of infection, select the check boxes by the file names and click **Clean**.

{button ,PI('gd.hlp',`CheckUp_Clean_Viruses_Clean_button')} Clean

{button ,PI('gd.hlp',`CheckUp_Clean_Viruses_Cancel_button')} Cancel

Select the check boxes by the names of the infected files and click **Clean**. After Guard Dog removes a virus, the file is safe to use again.

Click **Cancel** to return to the main CheckUp Found screen if you do not want Guard Dog to disinfect your infected files. However, do not open these files because a virus can spread to other files on your PC.

CheckUp Found - Files Containing Personal and Financial Information

Guard Dog checks all the files on your hard drive to see if they contain any information that you entered in Identity Protector and lists them in this screen. Guard Dog also determines whether any of these files are being protected by File Guardian and selects them automatically. You can perform the following actions:

{button ,PI('gd.hlp','Protect_button_on_the_CheckUp_File_Guardian_Add_file_page')} Protect

{button ,PI('gd.hlp','Cancel_button_on_the_File_Guardian_Add_file_page')} Cancel

Select the check box by the file name and click **Protect** if you want to add any of the files in this list to the files that are protected by File Guardian.

Click **Cancel** to return to the Checkup Found screen if you don't want File Guardian to guard these files.

CheckUp Status

Guard Dog is in the process of running a CheckUp based on the information that you gave Guard Dog during the Interview and any settings you may have entered in Customize CheckUp. As Guard Dog works, it highlights each check as it goes along and indicates progress in the status bar at the bottom of the screen. Additional information about the checks is provided in the More Information box on the right. You can click **Cancel** to stop the CheckUp at any time.

ActiveX

Active X is a technology used by software developers to implement controls in a program. An ActiveX control can add something as simple and useful as a button in a program's interface. Most of these good controls have been signed, meaning that they are harmless and will do nothing bad to the data on your computer. However, less than honest people use ActiveX technology to write programs that can jeopardize the security of the data on your computer, such as a program which searches your hard drive for certain file types and sends the information in it someone else.

Alert

When potential security risks or privacy violations occur, Guard Dog displays information about the impending risk in an alert dialog box. The alert contains information about what is happening and gives you options for dealing with the situation. Additionally, if your computer has a sound card installed, Guard Dog barks to indicate the presence of a potential security threat.

Bookmark

A bookmark is a convenient means of connecting to a Web site without typing in the URL. As you browse the Internet, you can bookmark those sites that you want to return to frequently. In some browser terminology this also can be referred to as adding a Web site to your “Favorites”.

Boot sector

To successfully write information to and read it from your hard drive, your computer's operating system needs to know about the type of file system installed on your hard drive, for example: FAT16, FAT32, or NTFS, and how the hard drive is physically organized into tracks, sides, and sectors. That information, and a lot more, is located in the boot sector on your computer's hard drive.


Browse

Those of us who frequently use the Internet usually connect to more than one Web site while we are connected. Navigating from site to site is generally referred to as browsing. Another popular term for the same activity is surfing.

Browser

A browser is a program like Netscape Navigator or Microsoft Internet Explorer that allows you to view text and graphics and to download files from Web sites on the Internet.

Browser Buddy

Browser Buddy is convenient tool with a dual purpose. First, Browser Buddy lets you view a summary of cookie activity. Just choose a Web site that you have visited from the drop-down list. Second, Browser Buddy gives you access to the passwords that you have stored in Password Manager. When you log on a password-controlled Web Site, you can drag and drop a user name and password from Browser Buddy to the appropriate box in the login form. To access Browser Buddy, right-click the Guard Dog icon  in the system tray and click **Browser Buddy** in the pop-up menu.

Cache

A cache is a reserved space on your computer's hard drive where programs like browsers store information. Your browser might store copies of visited Web pages and the images on those pages in a cache so that the next time you visit the page, it loads quickly because the browser uses the copies stored on your drive, instead of downloading the pages from the Web site.

Cookie

A cookie is a general mechanism that Web sites can use to both store and retrieve information about you. Cookies are placed on your computer by your browser as you browse the Internet. Generally, you are not made aware that this is happening and dozens of cookies can be written and read during one browsing session.

Cookie Blocker

Guard Dog's cookie protection functions are grouped together under the Cookie Blocker function. To access Guard Dog's Cookie Blocker settings, click **Options**, and then click **Protection Settings**. Select **Cookie Blocker** to display the **Cookie Blocker Protection Settings** page in the right pane of the dialog box.

Direct or indirect sites

A direct site is any location on the Internet that you visit simply by typing in the address (also known as the Universal Resource Locator or URL) for the site, or visit by clicking a hyperlink that connects one Web site to another. An indirect site monitors other sites. You never connect to it directly, but information about you can be passed from a site that you visit directly to the indirect site.

Domain name

Just as most houses are assigned numbers to help locate them on a particular street, the computers that make up the Internet also are identified by numbers. Because words are easier for most of us to remember than a long string of numbers, a name is assigned to a computer as well.

When you connect to a Web site, you do so by entering the full address of the computer that hosts the Web site you want to connect to. Part of that full address, more commonly known as the Universal Resource Locator (URL), is the domain name.

A domain name is composed of words separated by periods before the 3-letter top level extension and the extension itself, for example:

usatoday.com or espn.sportszone.com or yahoo.com

When you type an address, you can enter either the domain name or the number (if you know it). If you enter the name, another computer converts that name to the correct number.

DOS

At its most basic level, a computer's operating system simply contains instructions that tell the computer what to do. However, included in these instructions are fairly complex tasks, such as sending data to your printer or storing data on your computer's hard drive. Microsoft Windows has become a dominant operating system in the computer market place today. Even though the Windows operating systems are independent systems, they still depend on functions provided in an older Disk Operating System called DOS. To work with DOS, the you must familiar with a load of commands. Each one of these must be typed on the command line before the command can execute.

Some viruses such as boot sector viruses, partition table viruses, and memory viruses can infect files before Windows loads. For that reason, Guard Dog's Virus Sentry can scan for and identify those types of viruses using DOS before Windows loads. Also, if you make an Emergency Disk, the disk will contain a program that allows you to load DOS and run it on your computer if something happens to Windows.

Encryption

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.

On the Web, 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.

Executable file

An executable file is one that contains all the information necessary to start and run a program on your computer. When you click a program name on the Windows Program menu, you are really activating a shortcut to the program's executable file. Often a small program has all its files compressed into one executable file. Large programs can have many files, but the executable file will always be used to start the program. You can recognize an executable file because it has a .exe file extension. An executable file is often called a program file or a program executable file.

File extension

Some applications, for example: word processing, graphics, and spreadsheet programs, allow you to create files that are stored on your hard disk. When you save your file, The application asks you to enter a name and automatically appends three letters, called a file extension, after the name. Sometimes the application offers you a choice of file extensions. These three letters associate the file with the application so that if you want to view or edit the contents, you can open the file in the application that you used to create it.

File Guardian

Guard Dog's File Guardian can alert you when certain potentially harmful events occur as you use your computer, for example, ActiveX activity. Another important File Guardian feature is the **Guarded Files** list. You can place files in this list and indicate the applications that can use these files, thus ensuring that only the applications that you use to create or edit files can access the data in them. If an unauthorized program tries to access a file in the **Guarded Files** list, File Guardian will alert you. To access File Guardian settings, click Options, and click **Protection Settings**. Click **File Guardian** to display Guard Dog's **File Guardian Protection Settings** page in the right pane of the dialog box.

Gatekeeper

Guard Dog's Gatekeeper keeps an eye on which programs can access your sensitive files, and can automatically block file activity that seems suspicious. To access Guard Dog's **Gatekeeper** settings, click **Options**, and then click **Protection Settings**. Click **Gatekeeper** to display Guard Dog's **Gatekeeper Protection Settings** page in the right pane of the dialog box.

Harmful Web site

A harmful Web site is one that has content, such as viruses, ActiveX controls, or Java applets that are known to have harmful consequences when downloaded to your computer.

History

While you are using the Internet, the browser software collects the Universal Resource Locators (URLs) of all the Web sites that you visit and puts them in a file on your hard drive. For your convenience, most browsers have an option that lets you view these URLs; so that you can easily connect to a Web site by selecting the URL.

HTML

Acronym for Hypertext Markup Language, the language used to author or create documents on the World Wide Web.

HTTP

Acronym for HyperText Transfer Protocol, the system that undergirds the World Wide Web. HTTP specifies the way messages are formatted and transmitted, and how Web servers and browsers should respond. When you enter a Web address in your browser, it sends an HTTP request to your ISP's Web server, asking to access the Web site you requested.

Identity Protector

Guard Dog's identity protection functions are grouped together in the Identity Protector feature. As you use the Internet, Guard Dog will alert you if a program tries to send some of the information in Identity Protector to another location. To access Guard Dog's Identity Protector settings, click **Options** and then click **Protection Settings**. Click **Identity Protector** to display the **Identity Protector Protections Settings** page in the right pane of the dialog box.

Internet

The Internet and the World Wide Web are terms we use interchangeably to refer to the collection of computers that have been interconnected to form a network that spans the globe. Technically, the Internet is the collection of computers. The Web is the content on these computers, documents, graphics, files, and so forth. Usually, you connect your home computer to the Internet through an Internet Service Provider.

Internet Service Provider (ISP)

An Internet Service Provider (ISP) acts as a middle man between you and the Internet. Your computer connects using a modem) to the ISP's equipment which in turn connects to the Internet computers.

IP address

[See TCP/IP](#)

Java

Java is a tool for developing programs that run over the Internet. These small programs called “applets” can reside on a Web page. When a Java-enabled browser accesses a Web page containing Java applets, the browser downloads and runs the applets. Most applets are good, but there is no guarantee that they all are; and as a consequence, the data on your computer can be at the mercy of developers who design applets for unscrupulous purposes.

Memory

As you use your computer, frequently used data, that is stored permanently on your hard drive, is stored temporarily in a hardware device called memory so that it does not have to be retrieved from the hard drive each time it is needed. Memory device usage vastly improves the speed with which your computer can operate and if the information in memory is damaged, your computer won't run properly.

Modem

Modem is a word manufactured from two words—modulator and demodulator—that refers to a piece of computer hardware. The modem converts your computer's digital data into an acoustic format that can be easily transmitted over the telephone network. Another modem on the receiving-computer end converts acoustic data back to digital format. Modern modems are very flexible and can transmit data over a wide range of speeds. When establishing a connection, sending and receiving modems exchange signals—this process is called handshaking—to determine the transmission protocol to use for the session. If you have your modem configured with the sound on, you can hear the tones as they are exchanged through your computer's built-in speaker.

Partition table

You can divide your hard disk into sections called partitions. For example, you may need to run two operating systems on one computer. You could install each operating system, for example, Windows 3.1 and Windows 95 on its own partition. The partition table contains information about the size of each section and where it starts and ends on the hard drive.

Password Manager

Password Manager lets you store your various Web site login names and passwords in one secure location. When you are visiting a site that requires this information, you can drag it from Browser Buddy to the form displayed in your browser. To access Guard Dog's Password Manager settings, click **Options**, and then click **Protection Settings**. Click **Password Manager** to display Guard Dog's **Password Manager Protection Settings** page in the right pane of the dialog box.

Privacy Alert

Guard Dog displays a privacy alert dialog box whenever it intercepts a possible invasion of privacy on your PC.

Scheduler

A very helpful Guard Dog feature is the Scheduler which allows you to set up Guard Dog to perform certain time consuming tasks at times when you are not using your computer. To access Guard Dog's Scheduler settings, click **Options** and then click **Protection Settings**. Click **Scheduler** to display Guard Dog's **Scheduler Protection** settings in the right pane of the dialog box.

Search engine

A Web site designed to seek information on the Internet. Search engines consist of three basic components:

- 1 Form where you enter your query. For example, if you wanted to find out how goat cheese was made, you might enter the phrase "goat cheese production."
- 2 A database, containing an index of Web content. When you enter your query, the search engine examines its database, and returns the URLs of Web sites that it thinks are appropriate.
- 3 A "Webot," some automated method of probing Web sites for content. Since the Web is constantly changing, search engines must update their databases on a continuous basis. The Webot feeds its findings to the search engine's database.

Search Filter

Your Web browser can send your private search information to Web sites without your permission. Guard Dog's Search Filter can warn you before this happens. To access Guard Dog's Search Filter settings, click **Options** and then click **Protection Settings**. Click **Search Filter** to display Guard Dog's **Search Filter Protection Settings** page in the right pane of the dialog box.

Security Alert

Guard Dog displays a security alert dialog box whenever it intercepts a possible invasion of security on your PC.

Spam

Junk e-mail as well as junk Usenet postings. Another form of “spamming” is a malicious Internet attack, where a Web server is assailed with millions of spurious requests. Like regular junk mail, spam is frequently some form of advertising. Spam is not just a nuisance; it also wastes many Internet resources. Online services like America Online have begun to institute policies to keep spam from reaching their subscribers.

TCP/IP

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 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 for this, 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.

Trojan horse

A Trojan horse is a program that appears harmless until you download and install it on your computer. Then, it acts like a virus program.

Universal Resource Locator URL

Universal Resource Locator is the term applied to an Internet Web site address. The domain name is part of the address.

CyberMedia's URL is:

<http://www.cybermedia.com>

http—Is the method used to encode and transmit data between computers on the Internet.

www—Is the abbreviation for World Wide Web.

cybermedia.com—Is CyberMedia's domain name.

Virus

A virus is a program intentionally designed to affect your computer by attaching itself to a good program. While you use the program, the virus actively copies itself and attaches to other programs, thus infecting your computer like a virus infects the body. Most virus programs are just nuisances that take up disk space and cause programs to behave in unexpected ways. However, some virus programs can infect and seriously damage the files that your computer needs to start and load the operating system.

CyberMedia works constantly to identify viruses and find cures for them. CyberMedia places information about known viruses in a **virus pattern file**. As new viruses are identified the pattern file is updated with the new information. You can load the latest virus pattern file by using Guard Dog's Update feature.

Virus Alert

Guard Dog displays a virus alert dialog box whenever it detects a possible virus on your PC.

Virus Sentry

If you use the Internet extensively and download data from various sources, you run the risk of downloading viruses along with the data. Guard Dog provides extensive antivirus protection for the files and programs on your computer and can alert you when viruses are detected. To access Guard Dog's Virus Sentry settings, click **Options** and click **Protection Settings**. Click **Virus Sentry** to display Guard Dog's **Virus Sentry Protection** settings in the right pane of the dialog box.

Web site

The Internet and the World Wide Web are terms we use interchangeably to refer to the collection of computers that have been interconnected to form a network that spans the globe. Technically, the Internet is the collection of computers. They are owned by educational institutions, companies, the U.S. government, and so forth. The owners sell space on their computers to anyone who wants it and can afford it. This space and the content (documents, graphics, and so forth stored there) become a Web site and can be subdivided even further. The most common way to connect to a Web site is to enter the URL in your browser program.

Web Trail Cleaner

Guard Dog's Web Trail Cleaner can automatically remove the Web files your Web browser leaves behind. To access Guard Dog's Web Trail Cleaner settings, click **Options** and then click **Protection Settings**. Click **Web Trail Cleaner** to display Guard Dog's **Web Trail Cleaner Protection Settings** page in the right pane of the dialog box.

World Wide Web

The World Wide Web and the Internet are terms we use interchangeably to refer to the collection of computers that have been interconnected to form a network that spans the globe. Technically, the Internet is the collection of computers. They are owned by educational institutions, companies, the US government, and so forth. The owners sell space on their computers to anyone who wants it and can afford it. This space and the content (documents, graphics, and so forth stored there) become a Web site and can be subdivided even further. The most common way to connect to a Web site is to enter the URL in your browser program.

Universal Resource Locator is the term applied to an Internet Web site address. The domain name is part of the address.

CyberMedia's URL is:

<http://www.cybermedia.com>

http—Is the method used to encode and transmit data between computers on the Internet.

www—Is the abbreviation for World Wide Web.

cybermedia.com—Is CyberMedia's domain name.

Using the Guard Dog Glossary

The Guard Dog Glossary provides definitions for some common terms used in the Guard Dog Help system.

To see a list of the definitions:

- 1 Click Index.
- 2 Click in the list and scroll up and down.
- 3 If you are looking for a specific word, type the first few letters in the box. The Index scrolls automatically to the word that most closely matches what you type.

Gatekeeper Security Alert- Program launches another program

When you select the **Program tries to launch another program** check box in the Gatekeeper Protection Settings page, you will receive an alert message when Gatekeeper detects a program with Internet access privileges trying to access or run another program on your computer. You can use the options in the alert dialog box to allow or prevent access.

Why is this a risk?

Programs, in particular unfamiliar programs with Internet access can be a security risk because they can send private data someplace you probably don't want it to go.

How should I answer?

The following information should help you make a decision:

- **Allow Always**—Choose this if you intentionally ran the program that has Internet access and want it to be able to run the other program in the future without alerting you.
- **This Time Only**—Choose this if you are seldom going to use the application. Or, if you aren't sure whether this application should be allowed to launch the program in question, you may want to click **This Time Only** and proceed carefully.
- **Not This Time**—Choose this if you did not intentionally run this application, and you do not recognize it. At your earliest opportunity, you should locate the application on your computer and decide whether you really want to keep it.

Gatekeeper Security Alert - Browser connecting to a harmful site

When you select the **Going to harmful sites** check box in the Gatekeeper Protection Settings page, you will receive an alert message when Gatekeeper detects that you are connecting to a Web site that is known to have harmful active content, such as harmful ActiveX controls, hostile Java applets, or viruses.

Why is this a risk?

Connecting to a site that is known to have harmful controls, viruses, or Trojan Horses isn't wise. Having an ActiveX control or Java applet on your computer is a security risk because the program, which you really know nothing about, can do something that you may not want it to do. Viruses and Trojan Horses can be harmful to files on your PC.

How should I answer?

Close your browser immediately to prevent content from the harmful Web site from being downloaded to your computer. The longer you are connected to the Web site, the greater the chance that it can inflict damage on your PC.

- **Continue**—Choose this only if you are not concerned about the potentially harmful content on this Web site.

Gatekeeper Security Alert- Program trying to connect to the Internet

Each time a program tries to access the Internet, Guard Dog alerts you. You can use the options provided in the alert dialog box to control which programs have Internet access.

Why is this a risk?

You should become familiar with the trustworthy programs on your computer, which require access to the Internet to do their jobs. Examples of these are your Internet browser or a financial program that you use to pay your bills electronically. When another program that you are not familiar with attempts to connect to the Internet, you should scrutinize it carefully. It may be trying to send your sensitive data somewhere you don't want it to go.

How should I answer?

The following information should help you make a decision:

- **Allow Always**—The first time you use a new Internet program that Guard Dog has not seen before, an alert message is perfectly normal. You should choose **Allow Always** if you intend to use this program frequently. If you choose this option, Guard Dog adds the name of the program to the list of programs allowed to use your Internet connection in the Gatekeeper Protection Settings page. If you change your mind, you can always remove the program from the list.
- **Not This Time**—If you did not intentionally start this program or you do not recognize it, you should choose No. You should make a note of the program's name so that you can take the earliest opportunity to find the program and decide whether you really want to keep it.
If you did not intentionally start the program but you recognize it, you may want to choose **Not This Time** until you can investigate why it started.
- **This Time Only**—If you are trying out a new program but are not completely comfortable with it, you may want to choose **This Time Only**. This selection allows you to evaluate the program's performance before authorizing permanent access to the Internet.

What if I change my mind?

If you allow a program to access the Internet then you change your mind, you should:

- Quit the application.
- Remove the program from the list of programs allowed to use your Internet connection in the Gatekeeper Protection Settings page.

Gatekeeper Security Alert - Credit card number sent to an unsecure site

When you select the **Any credit card number goes out** check box in the Gatekeeper Protection Settings page, you will receive an alert message when Gatekeeper detects that a program is sending out a number that resembles a credit card number over an unsecure Internet connection. (Identity Protector provides added credit card protection, by watching for specific credit card numbers that you enter directly into the Identity Protector page in Protection Settings.)

Most companies that conduct business over the Internet provide a secure connection to their server so that you can engage in business transactions safely. When sending to a secure site, you may rest assured that some unscrupulous party cannot pick up the number. Because a secure site can have its own connection problems, most sites give you the option of using a secure or unsecured means of data transmission.

See the following topic for more information about secure connections.

[Some things you should know about privacy and security](#)

Why is this a risk?

If you send anything over an unsecured connection, there is always the possibility that someone can intercept your data and use it for their own purposes.

How should I answer?

- **Not This Time**—Choose this if you want to prevent your credit card number from being sent out over an unsecure connection at this time.
- **This Time Only**—Choose this if you are willing to accept the risk just this once.

File Guardian Security Alert - Attempt to format hard disk

Warning!

If you did not intend for your disk to be formatted, turn off your computer now using its power switch.

File Guardian is your computer's watchdog. Some of the programs that you install on your computer may come from less than reliable sources. You really can't tell what a program is going to do until you install and use it. Something that is seemingly innocent may be designed to do something destructive, like Trojan horse programs which can reformat your hard disk. File Guardian can protect you from this menace.

Why is this a risk?

Reformatting a hard disk is not a task that you undertake lightly. You are effectively removing everything—operating system, data, and applications— from the drive and starting from square one. If a program does this unexpectedly without your permission, you run the risk of losing everything on your hard disk.

How should I respond?

Shut your computer down NOW using its power switch if you don't know why your disk is being formatted. Click **Ignore** if you (or a program you are using) intentionally started the format operation.

File Guardian Security Alert - Program accessing file

After you add a file to the **Guarded File** list in the File Guardian Protection Settings page, you will receive an alert message when an unauthorized application tries to access the file. You can use the options in the alert dialog box to determine whether the application can access the file. You can choose:

- **Allow Always**—The application can have access to the file.
- **Not This Time**—The application cannot access the file this time.

How should you answer?

The following information should help you make a decision:

- If you intentionally run an application that normally uses this file, click **Allow Always** and restart the application if necessary. This is a good choice if you intentionally try to open up a guarded file from within an application and expect to do so again.
- If you did not intentionally run this application, and you do not recognize it, click **Not This Time** on the alert dialog box. At your earliest opportunity, you should locate the application on your computer and decide whether you really want to keep it.

Cookie Blocker Privacy Alert - Sending cookie from direct Web site

Generally speaking, a direct site is one you connect to by typing in the URL or by clicking a link in your browser. As you navigate through the Internet, Web sites send cookies to and receive them from your browser. Cookies can help a Web site better serve you by using information it has previously obtained and stored on your computer. For example, cookies can allow your favorite merchandising site to display custom information for you each time you visit, or allow a password-protected Web site to retrieve your password so that you don't have to enter it each time you visit the site. Based upon the selections you made in Cookie Blocker Protection Settings page, Guard Dog alerts you when a Web site that you connect to directly tries to exchange cookies with your computer.

Why is this a risk?

Because you have no control over what is being tracked or who is collecting information about you, cookies can pose a threat to your privacy.

How should I respond?

- **Accept Always**—Choose this if the site you are connecting to requires cookies for proper operation or if you visit the site frequently and trust it. Guard Dog adds this site to the Allowed list in the Cookie Blocker Protection Settings page. The next time you visit this site, Guard Dog accepts the site's cookies automatically.
- **Never Accept**—Choose this if you don't visit this site very often, or if you don't want this site to recognize you. Guard Dog adds this site to the Rejected list in the Cookie Blocker Protection Settings page. The worst thing that can happen is that you won't be able to view pages from this site until you remove it from the Rejected list.

What if I change my mind?

If you change your mind about a site, you can switch sites from **Allowed** to **Rejected** and vice versa in the Cookie Blocker Protection Settings page. If you want a fresh start, remove the site from either list—the next time you visit the site and it tries to set a cookie, Guard Dog will alert you. Also available on this page are options that allow you to control Cookie Blocker behavior based on Direct and Indirect sites.

Cookie Blocker Privacy Alert - Sending cookie from indirect Web site

Generally speaking, an indirect site is one that you do not connect to by typing in the URL or by clicking a link in your browser. For example, if you connect to a site that displays information in frames, the information in a frame may be coming from another Web site. (Depending on your browser, you may be able to see the other sites's Web address by positioning your cursor over the frame and looking at the information in your status bar.)

As you navigate through the Internet, Web sites send cookies to and receive them from your browser. Cookies can help a Web site better serve you by using information it has previously obtained and stored on your computer. For example, cookies can allow your favorite merchandising site to display custom information for you each time you visit, or allow a password-protected Web site to retrieve your password so that you don't have to enter it each time you visit the site. Based upon the selections you made in Cookie Blocker Protection Settings page, Guard Dog alerts you when a Web site that you connect to indirectly tries to exchange cookies with your computer.

Why is this a risk?

You may not be aware that you have come in contact with an indirect Web site. Because you have no control over what is being tracked or who is collecting information about you, cookies can pose a threat to your privacy.

How should I respond?

- **Never Accept**—Choose this if you don't visit this site very often, or if you don't want this site to recognize you. Guard Dog adds this site to the Rejected list in the Cookie Blocker Protection Settings page. If the site requires cookies, the worst thing that can happen is that you won't be able to view pages from this site until you remove it from the Rejected list.
- **Accept Always**—Choose this if the site requires cookies for proper operation or you visit the site frequently and trust it.

What if I change my mind?

If you change your mind about a site you can switch sites from Allowed to Rejected and vice versa in the Cookie Blocker Protection Settings page. If you want a fresh start, remove the site from either list—the next time you visit the site and it tries to set a cookie, Guard Dog will alert you. Also available on this page are options that allow you to control Cookie Blocker behavior based on Direct and Indirect sites.

File Guardian Alert - ActiveX scanning files

When you select the **ActiveX scans my drive** check box in the File Guardian Protection Settings page, you receive an alert message when File Guardian detects an ActiveX control scanning files on your hard drive.

Why is this a risk?

A Web site can download ActiveX controls to your computer without your knowledge. Because a control can run on your computer just like a program that you have installed, it can do things that you might not want it to, such as gather personal data and sent it to another computer. There are legitimate reasons for allowing an ActiveX control to read through all of your files. For example, if you visit a virus detection Web site, it would need to read your files in order to find a virus. However, if a site scans your files without warning you, you need to think about whether you trust the site.

How do I respond?

- **This Time Only**—Choose this only if you trust the control and feel that it is not scanning your disk with intent to harm your data.
- **Not This Time**—Choose this if you suspect that the control is going to do harm.

File Guardian Security Alert - ActiveX deleting files

When you select the **ActiveX deletes files from my drive** check box in the File Guardian Protection Settings page, you receive an alert message when File Guardian detects an ActiveX deleting files from your hard drive.

Why is this a risk?

A Web site can download ActiveX controls to your computer without your knowledge. Because a control can run on your computer just like a program that you have installed, it can do things that you might not want it to, such as delete files. There are legitimate reasons for allowing an ActiveX control to delete files. For example, if you visit a site regularly and it tells you that it needs to update software that it uses to provide you a service, it may need to delete outdated files.

How do I respond?

- **This Time Only** –Choose this only if you trust the control and feel that it is not deleting files with intent to harm your data.
- **Not This Time**–Choose this if you suspect that the control is going to do harm.

Web Trail Cleaner Privacy Alert

Web Trail Cleaner alerts you based on the selections you make on the Web Trail Cleaner Protection Settings page. Thus, if you select **Prompt to Clean Up after closing Web Browser** in the Web Trail Cleaner Protection Settings page, you receive an alert dialog box each time you close your Web browser. (If you are using Microsoft Active Desktop, you will only see this dialog box when you shut down Windows, as Internet Explorer does not shut down entirely until Windows shuts down.)

See the following topic for more information about Web Trail Cleaner protection settings.

[About Web Trail Cleaner](#)

Why is this a risk?

As you browse the Internet, the URLs that you have visited are stored on your computer along with images and pages that Web sites use to make loading their content faster. If other people use your computer, you may want to protect your privacy by deleting a record of your browsing activity. Guard Dog deletes files for selected Web sites from the following folders:

- **Cache**–Web sites store pages and images in the cache folder and use them when you revisit the site to speed up the loading process.
- **URL**–Your browser stores the URL that you have visited in this folder and displays the most recently visited URLs.
- **History**–URLs are stored here too. Your browser removes entries from this folder periodically.

Note

The folder names may be different depending upon the browser you are using.

How should I answer?

Guard Dog automatically selects sites that you haven't bookmarked or added to your list of favorite sites. Since most people create bookmarks for sites they return to, Guard Dog assumes that you might want to keep browsing information for these sites.

- **Clean**–Choose this to remove evidence of your Internet browsing related to the selected sites. Removing these files does not harm the operation of your computer. It's really up to you and the amount of space available on your hard drive whether you keep these files or not.
- **Don't Clean**–Some people like to keep history files so that they can find an interesting Web site that they may have forgotten to Bookmark or add to their Favorites list in their browser.

Tip

You can sort the sites in the list by clicking a column heading. To select sites that are adjacent to each other in the list, click the first site, hold down the SHIFT key and click the last site. To select non-adjacent sites, hold down the CTRL key and click sites each site. When you select or clear the check box for any site in the selection, Guard Dog matches the check box state for all selected sites.

File Guardian Security Alert - Windows password file being accessed

When you select the **Password files are accessed** check box in the File Guardian Protection Settings page, Guard Dog alerts you if a program tries to access any Windows password (.PWL) file.

Why is this a risk?

Windows password files store your Windows passwords, allowing you to connect automatically to password-protected resources, such as a network drive, without having to type the password each time. If an unknown program is trying to gain access to this file, the data contained in this file may be in danger.

How should I respond?

- **This Time Only**—Choose this if you recognize and trust the program. If you are unfamiliar with the program and want to allow access, watch your password-protected resources for any suspicious activity.
- **Not This Time**—Choose this if the program is foreign to you, or you have reason to be suspicious of it.

Identity Protector Privacy Alert - Personal or financial information being sent

You entered information that you considered important in Identify Protector. When Guard Dog detects that your browser is about to send part or all of this information to a Web site, Guard Dog alerts you.

Why is this a risk?

There are many enterprising businesses that collect your name, address, and e-mail address to sell to other businesses. Mostly your information goes on mailing lists and you receive a lot of junk mail or e-mail. However, your personal information could fall into the wrong hands. For example, someone could use your e-mail address to send obscene jokes to a mailing list or financial information could be used to try to gain access your bank, loan, or securities accounts.

How should I respond?

- **This Time Only**—Choose this if you trust the site to which your browser is sending the information. If the site is using a secure connection, others can't intercept this information.
- **Not This Time**—Choose this if you do not trust the site. You may also want to consider blocking this information if it is not being sent over a secure connection.

See the following topic for information about how secure Internet connections are implemented.

[Some things you should know about privacy and security](#)

Virus Alert - Virus found

Guard Dog's Virus Sentry scans files based on the choices you made in the Virus Sentry Protection Settings page. Guard Dog alerts you when it detects that a virus has infected one of the file types you have specified.

Why is this a risk?

Viruses are mostly nuisance programs that attach themselves to other programs, take up space, and cause these programs to behave strangely. However, there are very hostile viruses that can do real damage to the files that your computer needs to run properly. Any virus can place the data on your hard drive at risk.

How should I respond?

- **Clean**—Choose this if you want Virus Sentry to remove the virus from the file. If the virus has irreparably damaged the file, Virus Sentry will offer to delete the file.
- **Don't Clean**—Choose this if you want Guard Dog to take no action. Do not open the file or you risk spreading the virus.

Gatekeeper Security Alert - Modem dialing silently

When you select the **My modem dials silently** check box in the Gatekeeper Protection Settings page, Guard Dog alerts you when it detects that your modem is dialing with the sound turned off.

Why is this a risk?

You could have a program on your computer, unbeknownst to you, that can make long distance calls or even call another computer and transmit data to it.

How should I respond?

- **Not This Time**—Choose this if you do not know why your modem is dialing.
- **This Time Only**—Choose this if you know the calling destination, for example, you may be dialing your Internet Service Provider to make a connection to the Internet.

Scheduler Guard Dog Alert - Update notification

Guard Dog has an event set up in the Scheduler Protection Settings page to remind you to check for updates for Guard Dog. A new virus pattern file, which keeps your Guard Dog AntiVirus protection current, is available each month. An update to the Guard Dog program may also be available.

How should I respond?

- **Update**—Choose this to have Guard Dog retrieve and install the update. You should keep Guard Dog up-to-date with the latest virus patterns, fixes and enhancements to ensure that your PC is receiving the best protection possible.
- **Ignore**—Choose this if you don't want to update Guard Dog at this time.

Tip

Guard Dog uses CyberMedia's Oil Change technology to locate and download updates from the CyberMedia Web site. If you did not install Oil Change when you installed Guard Dog, you should do so now. This program is located on the Guard Dog installation disc.

Scheduler Guard Dog Alert - Create or update your Emergency Disk

You have scheduled an event in the Scheduler Protection Settings page to remind you to create an Emergency Disk, or to update the information on an existing set of disks that you have already created.

How should I respond?

- **Create**—Because you can't predict when disaster will strike your computer, you should create or update your Emergency Disk to ensure the highest level of protection.
- **Ignore**—Click **Ignore** to dismiss the alert without taking action on the reminder.

About Guard Dog Preferences

You can control basic Guard Dog features and actions by selecting the options on the Preference Protection Settings page.

In the **At Startup** group box, you can select:

- **Load Guard Dog**—Starts Guard Dog monitoring your computer for potential problems when Windows starts. It is important to load Guard Dog at this time because some viruses can attack the files that your computer needs to load the Windows operating, and Guard Dog can alert you when this type of danger is present.
- **Show Splash Screen**—Displays briefly the Guard Dog logo.
- **Use Password**—Protect your settings from unauthorized changes by assigning a password to the Guard Dog program. You will enter the password each time you start your computer.

In the **Sound Effects** group box, you can select:

- **Sound Effects**—Determine the sound Guard Dog plays when it displays a Privacy, Security, or Virus Alert message.

Click the Speaker button to play the selected sound.

How do I set Guard Dog Preferences?

- 1 Click **Options** in the Guard Dog Home screen. Then click **Protection Settings**.
In the left side of the screen, make sure that a check appears in the check box next to Preferences.
- 2 Select the following check boxes:
 - Load Guard Dog**
 - Show the Splash Screen**
 - Use Password/Change Password**—During the Interview you may have chosen a password for Guard Dog. If you did, you can click **Change Password** to choose a different one. If you did not assign a password and you select **Use Password**, the button is **Set Password**.
- 3 If your computer is equipped with a sound card, you can also choose a distinctive bark for each type of alert.
 - Privacy Alert**
 - Security Alert**
 - Virus Alert**
- 4 Click the arrow beside each list box and choose one of the following alerts:
 - Quiet**
 - Bark**
 - Double Bark**
 - Growl**
- 5 Click **OK** to have Guard Dog save your selections.

Tip

To get a preview of the bark you selected, click the speaker by the appropriate list box.
See the following topic for more information about alerts.

[Responding to Guard Dog alerts](#)

About Scheduler

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 thorough virus check while you are away from your computer. Remember to leave your computer on, during the scheduled time period.

You can schedule the following tasks

- **A virus check on all files**– Check for viruses in all files on all local drives, including floppy drives, CD-ROM, and removable media drives.
- **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 removable media drives. By default, this check is scheduled to occur automatically when Windows starts.
- **A virus check on changed files**–Perform a virus check only on files that have been created or modified after the date and time that all files were last checked for viruses. (Virus Sentry will check all files if all files have never been checked.)
- **Encryption of files on my computer**–Encode files that are in the Guarded Files list of File Guardian.
- **Decryption of files on my computer**–Decode encrypted file that are in the Guarded Files list of File Guardian.
- **Schedule the removal of deleted files on my PC**–Write over data that remains after files are permanently deleted from your Recycle Bin.
- **Remind to create an Emergency Disk**–Display a reminder message. When you install Guard Dog, this event will be scheduled to occur every six months unless you change the frequency in the Emergency Disk Interview page.
- **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.

How do I set up a Schedule?

- 1 Click **Options** on the Guard Dog Home page. Then click **Protection Settings**.
- 2 In the left side of the screen, make sure that a check appears in the check box next to Scheduler.
- 3 Click **Scheduler**.
- 4 Click **Add**.
- 5 Select an event to schedule.
- 6 The Add Schedule Wizard will guide you through selecting an interval, date, and time for the event.
- 7 Click **Finish** to add the event to your Scheduler list.

To edit a Schedule

- 1 Select the event in the Scheduler list.
- 2 Click **Edit**. The Add Schedule Wizard will guide you through the selections.

To remove an event from the Schedule

- 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 CONTROL key and click each desired event.
- 2 Click **Remove**.

See the following topic for more information about checking for viruses.

[About Virus Sentry](#)

About Cookie Blocker

Cookies are small files that your Web [browser](#) stores on your computer 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 tag, which let the Web server track which pages you view and how often you return to them. For a more detailed description of cookies.

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

- Reject all cookies.
- Allow 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 send the cookie, and advises you whether 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 chose to 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 through a connected site's links. For example, an ad displayed in a separate frame in the page can come from a different site.

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.
- Automatically prevent cookies from being accepted from indirect sites.

How do I set Cookie Blocker settings?

- 1 Click **Options** on the Guard Dog Home screen and click **Protection Settings**.
- 2 Make sure that there is a check in the box by Cookie Blocker in the left pane then select Cookie Blocker. Guard Dog displays the Cookie Blocker Protection Settings page.
- 3 Choose the following for **Direct Sites**:

Accept to always accept cookies from sites that you connect to directly. As you browse the Web, Cookie Blocker adds these sites to the **Allowed** list.

Reject to refuse cookies from sites that you connect to directly. As you browse the Web, Cookie Blocker adds these sites to the **Rejected** list.

Prompt to choose whether to accept or reject a cookie from a direct site on a case-by-case basis. As you browse the Web, Guard Dog asks you each time a direct site tries to send a cookie to your computer.

Choose the following for **Indirect Sites**:

Accept to always accept cookies from sites that you connect to indirectly. Cookie Blocker adds these sites to the **Allowed** list.

Reject to refuse cookies from sites that you connect to indirectly. As you browse the Web, Cookie Blocker adds these sites to the **Rejected** list.

Prompt to choose whether to accept or reject a cookie from an indirect site on a case-by-case basis.

To remove cookies from the Allowed or Rejected lists

- ▶ On the Cookie Blocker Protection Settings page, click a site in either list and click **Remove**.

To move sites from one list to the other

- ▶ On the Cookie Blocker Protection Settings page, click a site and click the right (>>) or the left (<<) arrow.

What if I change my mind and want my old settings back?



Click **Default** to restore previous settings.

See the following topic for information about responding to a Cookie Blocker alert.

[Responding to a Cookie Blocker Alert](#)

About Identity Protector

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 stop an application from sending any personal information that you specify out over the Internet.

Although you don't have to worry about a site when you connect using a secure connection, there are many Web sites that use a secure connection only when dealing with credit card transactions. Guard Dog will warn you when financial information is being sent to non-secure site.

Also, 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 automatically replaces any protected personal information sent to an unsecure web site with x's. For example if your child tries to order the latest CD without entering your Guard Dog password, Guard replaces your credit card number with x's.

- 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. The alert message tells you , and advises you whether or not to let the information go out.

How do I set Identity Protector settings?

- 1 Click **Options** on the Guard Dog home screen and click **Protection Settings**.
- 2 Make sure that there is a check in the box in the left pane by Identity Protector then select Identity Protector. Guard Dog displays the Identity Protector Protection Settings page on the right.
- 3 In the **Personal Information** box do one of the following:
 - Click **Add** to display the wizard that helps you enter more personal information into Identity Protector.
 - Select a personal information item and click **Edit** to display a wizard that helps you change this item.
 - Select a personal information item and click **Remove** to delete the item from Identity Protector.
- 4 Follow the same procedure to Add, Edit, or Remove information In the **Financial Information** box.

See the following topic for more information about responding to an Identity Protector alert.

[Responding to an Identity Protector alert](#)

About Web Trail Cleaner

As you [browse](#) the [Internet](#), your [browser](#) stores information that makes your browsing experience more satisfying. It uses the information as follows:

- [Cached](#) files—Storing files on your computer speeds up the display of Web page elements such as graphics.
- [URL](#) visited—Lets you return to Web sites that you visited during the browsing session without entering the address again.
- History—URLs that you visit are stored for a specific length of time that is set in your browser's options.

Anyone using your computer can view these files 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, Web Trail Cleaner will automatically clean up your Web browsing trails. When you close your browser, Guard Dog displays the Web Trail Cleaner alert message.

How do I set Web Trail Cleaner settings?

- 1 Click **Options** on the Guard Dog home screen and click **Protection Settings**.
- 2 Make sure that there is a check in the box in the left pane by Web Trail Cleaner then select **Web Trail Cleaner**. Guard Dog displays the Protection Settings page on the right.
- 3 Choose one of the following options:

Prompt to clean up after closing Web browser—Choose this setting if you want Guard Dog to ask you each time close your browser.

Automatically Clean Up after closing Web browser—Choose this if setting if you want Guard Dog to clean the cache, history and URL folders each time you close your browser without asking you first.

Tip

When you select Automatically clean up after closing Web browser, you can ensure that Guard Dog does not delete the URLs to any sites that you have [bookmarked](#) or added to your favorites list by selecting the **Keep bookmarked items** check box. See the following topic for more information about responding to a Web Trail Cleaner alert.

[Responding to a Web Trail Cleaner alert](#)

About Search Filter

Search Filter prevents information that you provide to one Web site from being passed along to another site. Without Search Filter, such information is retained by your Web browser and can be extracted by the next site you visit.

If you have Search Filter selected in Protection 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.

How do I set Search Filter settings?

- 1 Click **Options** on the Guard Dog Home screen and click **Protection Settings**.
- 2 Make sure that there is a check in the box in the left pane by Search Filter.
There are no settings associated with Search Filter. It is either turned on or off.

About Gatekeeper

Gatekeeper lets you control which 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 number pattern.

How do I set Gatekeeper settings?

- 1 Click **Options** on the Guard Dog home screen and click **Protection Settings**.
- 2 Make sure that there is a check in the box in the left pane by Gatekeeper and select **Gatekeeper**. Guard Dog displays the Protection Settings page on the right.
- 3 Click in the check box by the warning you want to receive. Gatekeeper will warn you when:
 - You are about to connect to a harmful Internet site. A harmful site is one that has harmful active content such as [ActiveX](#) controls and Java applets.
 - The modem on your computer dials silently. It could be making a long distance call.
 - A program tries to launch another program. Some program could be trying to connect to the Internet.
 - Any credit card number goes out. You want to ensure that you are the only one sending out credit card numbers over the Internet.
- 4 There are some programs that you will always grant Internet access to and Guard Dog adds these programs to the list in the Gatekeeper dialog box. If you change your mind about access, just select a program on the list and click **Remove**.

See the following topics for more information about responding to Gatekeeper alerts.

[Responding to a harmful site alert](#)

[Responding to a silently dialing modem alert](#)

[Responding to an Program Launch alert](#)

[Responding to a credit card information alert](#)

About File Guardian

File Guardian can protect files containing your sensitive data from being opened, renamed, copied, moved, or deleted. Guard Dog can also alert you if a program attempts one of the following potentially harmful activities:

- A program attempts to reformat your hard drive—When a format command is started, Guard Dog doesn't know whether you told your computer to format a floppy 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 disk—such as Guard Dog creating an Emergency Disk.
- An ActiveX control attempts to delete files on your hard drive—There are legitimate reasons for allowing an ActiveX control to delete files. For example, if a control installs special software on your computer to let you interact with its Web site, the control may need to delete files that 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
- An ActiveX control attempts to scan files on your hard drive—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 Web site that uses an ActiveX control to look for viruses on your computer. 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.
- A program attempts to access your system password files.

How do I set File Guardian settings?

- 1 Click **Options** on the Guard Dog home screen and click **Protection Settings**.
- 2 Make sure that there is a check in the box in the left pane by File Guardian and select **File Guardian**. Guard Dog displays the Protection Settings page on the right.
- 3 Click in the check box by the warning you want to receive. File Guardian will warn you when:
 - ActiveX control scans your drive.
 - Your drive is being reformatted.
 - ActiveX control deletes files from your drive.
 - Your drive is being reformatted.

You tell File Guardian which files to guard on your hard drive and which programs can be used to open the files. Guard Dog adds or removes programs from the Guard Files list. If an unauthorized application attempts to access a guarded file, Guard Dog displays an alert message. 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.

To add files and programs to the Guarded Files list



On the File Guardian Protection Settings page, click **Add** to start the wizard that will help you add files and programs to the Guarded Files list.

[Encryption](#) is another protection feature of File Guardian. Adding encryption ensures that no other program can read the data in the protected files.

To encrypt or decrypt files in the Guarded Files list



As you go through the Add Guarded Files wizard you will be given the option to include a file for encryption. If you select this option, a lock icon appears by the file name. You can encrypt or decrypt all the marked files in the Guarded Files list by right-clicking the Guard Dog icon



on the system tray and selecting either **Encrypt File Guardian files** or **Decrypt File Guardian files**.

To remove files and programs from the Guarded Files list



In the File Guardian Protection Settings page, select a file in the Guarded Files list and click **Remove**.

See the following topics for information about responding to File Guardian alerts.

[Responding to ActiveX activity alert](#)

[Responding to a disk reformat alert](#)

[Responding to a password-protected file alert](#)

[Responding to an Program Launch alert](#)

About Password Manager

Password Manager lets you store your various Web site login names and passwords in one secure location. When you are visiting a 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 the list of stored login names and passwords.
- Add a password record.
- Edit a password record.
- Remove a password record.

You can also add a record in Browser Buddy.

See the following topic for more information about Browser Buddy.

[About Browser Buddy](#)


How do I use Password Manager to add a password record?

- 1 In the Guard Dog Home screen, click **Options**, then click **Protections 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 password 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**.

How do I use Password Manager to remove a password?

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

About Virus Sentry

You can use Virus Sentry to control which types of files CheckUp scans, as well as specify as-you-work virus checking options.

How do I control which files CheckUp scans?

- 1 On the Guard Dog home screen, click **Options** and select **Protection Settings**.
- 2 Make sure that the check box by **Virus Sentry** is selected in the left pane, then click **Virus Sentry**. The Virus Sentry Protection Settings page appears on the right.
- 3 In the **What to check** box, click the arrow by the drop-down list and select:
 - **All Files**—Checks every file on your computer. This is the most complete check, but also the most time-consuming check if you have a lot of files on your computer. It will catch viruses in files that use non-standard file types.
 - **Program Files**—Checks all files that a program requires in order to run. It checks files using the most common program file extensions, such as .com, .exe, .bat, .bin, .ovl, .drv, .dll, .sys, .tsk, .vxd, and .ocx. This setting will not catch macro viruses.
 - **Document Files**—Checks only data files that can contain viruses, which are typically macro viruses. For example, Microsoft Word and Excel document files, and file compression documents such as .zip, .arc, and .lzh. This setting will not catch program viruses.
 - **Program Files and Document Files**—Checks both program and document files. This setting will find most viruses and is less time-consuming than checking all files.
- 4 Click **Edit** in the **What to Check** box.
Guard Dog displays a wizard to help you choose types of files to check.

How do I set up as I work options?

- 1 In the Guard Dog Home screen, click **Options** then click **Protections Settings**.
- 2 Make sure that there is a check in the box in the right pane by **Virus Sentry** and click **Virus Sentry**. The Virus Sentry Protection Settings page appears on the right.
- 3 Select or clear the check boxes by the following options in the **When to check** box:
 - **Program execution**—Checks a program for viruses before it runs on your computer.
 - **E-mail access**—Checks e-mail messages before they are opened.
 - **File open**—Checks each time you open a file on your computer.
 - **Move or Rename**—Checks for viruses each time you move or rename a file.
 - **Floppy drive read**—Checks for viruses each time you read information from a floppy disk.
 - **DOS Startup**—Checks your computer's DOS startup process for boot sector or partition table viruses, which can only be cleaned in DOS. (This is a before-you-work option.)

To exclude files and folders from the CheckUp Virus Check



Click **Add Files** or **Add Folders** in the **Do not check these files in these folders** box and make your selections.

Tip

Guard Dog references the **Do not check these files in these folders** list during CheckUp and during any scheduled virus check, but does not use the list when checking files based on what you selected in the **When to check** box.

To remove files and folders from the exclusion list



Click an entry in the **Do not check these files in these folders** box, and click **Remove**.
See the following topic for more information about responding to a Virus Sentry alert.

[Responding to a Virus Sentry alert](#)

Responding to Guard Dog Alerts

Based on the Protection Settings that you have chosen, Guard Dog monitors your computer and alerts you when certain things happen that could have harmful results. The alert provides information about what caused the [alert](#) and offers options for dealing with the situation.

During the first few computing sessions after you have installed Guard Dog, these alerts may be a little disruptive. However, we ask you to be patient and carefully answer the questions posed by Guard Dog.

See the following topics for information about responding to the different alerts.

[Responding to an Program Launch alert](#)

[Responding to a harmful site alert](#)

[Responding to an Internet Access alert](#)

[Responding to a credit card information alert](#)

[Responding to a disk reformat alert](#)

[Responding to a silently dialing modem alert](#)

[Responding to a Cookie Blocker alert](#)

[Responding to ActiveX activity alert](#)

[Responding to an ActiveX control deleting files](#)

[Responding to a Web Trail Cleaner alert](#)

[Responding to a password-protected file alert](#)

[Responding to a personal information alert](#)

[Responding to a Virus Sentry alert](#)

[Responding to an Update Notification alert](#)

[Responding to an Emergency Disk reminder alert](#)

Getting the most from AntiVirus protection

Your computer is under threat of [virus](#) attack from many sources, for instance, when you access an infected floppy disk, open an infected e-mail attachment, or download a virus-infected program from the [Internet](#). Using strong AntiVirus protection—like that available in Guard Dog—keeps your PC virus free. Guard Dog offers you several ways to check for and get rid of viruses. Initially during the Interview, you can set up virus checking by selecting:

- **Whenever Windows starts up**—Guard Dog automatically checks high-risk files (document files and program files) when Windows starts.
- **Automatically whenever there is some file activity or download**—Guard checks for virus upon:
 - Program execution
 - Email file access
 - File open
 - Move or Rename
 - Floppy drive read

After the Interview you can:

- **Check your program and document files using CheckUp**— After you install Guard Dog, run CheckUp to have the AntiVirus feature thoroughly check the program and document files on your local drives for virus infection. After running a complete scan the first time, you may want to adjust your CheckUp virus settings.

See the following topic for more information about setting up AntiVirus protection during CheckUp.

[How to check for viruses during CheckUp](#)

- **Schedule different virus checks**—Checking for viruses can take some time if you have a large amount of data on your PC. You can set up a schedule for a time when you aren't using your computer.

See the following topic for more information about setting up a schedule for AntiVirus protection.

[How to set up a schedule for virus checking](#)

- **Check a specific folder**—You may want to check only the files in one folder.

See the following topic for more information about checking the files in a selected folder.

[How to check files in one folder](#)

- **Check using the as-you-work options in Virus Sentry Protection Settings**—You find several options in Virus Sentry Protection Settings that allow you to check for viruses while you are using your PC.

See the following topic for more information about selecting as-you-work options in Virus Sentry

[How to select options in Virus Sentry](#)

How to check for viruses during CheckUp

If you use shareware or receive files from unreliable sources, Virus Check is an indispensable weapon in your defense against virus attack. The Virus Check option lets you specify what to check when you run a CheckUp.

How do I set up AntiVirus protection during CheckUp?

This is a two-step process:

First Step—Select which drives and folders to check

- 1 On the Guard Dog home screen, click **Options** and select **CheckUp Settings**.
- 2 To check all folders on all drives, select the check box by **My Computer**. Checks appear by all drives and folders in the list.
- 3 To select drives and folders individually, clear the check box by **My Computer**, then select each check box by the drive and folder.

For example, select the check box by c: and checks appear by all the folders listed under c: Clear the check boxes by the folders that you don't want Guard Dog to check for viruses.

Second step—Select what to check

- 1 On the Guard Dog home screen, click **Options** and select **Protection Settings**.
- 2 In the left pane of the **Protection Settings** dialog box, make sure that a check appears in the check box by **Virus Sentry**, then select **Virus Sentry**.
The Virus Sentry Protection Settings page appears on the right.
- 3 In the **What to Check** group box select one of the following from the drop-down lists:
 - **All Files**—Checks all file types the folders you selected in the First Step.
 - **Program files**—Checks only program-related files in the folders you selected in the First Step.
 - **Document files**—Checks in the folders you selected in the First Step.
 - **Program and Document**—Checks both program-related files and document files in the folders you selected in the First Step.
- 4 Click **Edit** in the **What to Check** box.
Guard Dog displays a wizard to help you choose document files types and program files types to check.

Tip

If you have any questions about how to use the wizard, click **Help** on any of the wizard screens or press **F1** on your keyboard. Guard Dog displays information specifically designed for the wizard page that is displayed.

As you use CheckUp, you may want to exclude files and folders from Virus Check, for example when you check large file groups and you know that some files contained in the group are virus free. You can add them to the **Do not check these files and these folders** in Virus Sentry.

Optional Step—Specify what NOT to check in during CheckUp

- 1 On the Guard Dog home screen, click **Options** and select **Protection Settings**.
- 2 In the left pane of the **Protection Settings** dialog box, make sure that a check appears in the check box by **Virus Sentry**, then select **Virus Sentry**. The Virus Sentry Protection Settings page appears on the right.
- 3 In the **Do not check these files and these folders** select what you want to exclude by doing the following:
 - Use **Add Files** to open the **Add File** dialog box navigate to a specific file.
 - Use **Add Folders** to open the **Browse for Folder** dialog box and navigate to the folder.

How to set up a schedule for virus checking

If you want to scan your PC for viruses without running CheckUp, Guard Dog lets you set up a scheduled virus check. Scheduling can be particularly useful if you have large amounts of data on your PC. You can select what to check and the type of check to run and set up a schedule for the check so that it occurs at a time when you aren't using your PC. By default, Guard Dog sets up two scheduled Virus checks: high-risk (program and document) files each time you start windows and all files each month.

How do I change AntiVirus protection for scheduled virus checks?

This is a two-step process:

First Step—Select which drives and folders to check

- 1 On the main Guard Dog screen, click **Options** and select **CheckUp Settings**.
- 2 To select drives and folders individually, clear the check box by **My Computer**, then select each check box by the drive and folder.
For example, select the check box by **c:** and checks appear by all the folders listed under **c:**. Clear the check boxes by the folders that you don't want Guard Dog to check for viruses.

Second Step—Select what to check and set up a schedule

Note

One of the advantages of using the Scheduler Wizard is that you can skip selecting **What to check** in the Virus Sentry Protection Settings page.

- 1 On the main Guard Dog screen, click **Options** and select **Protection Settings**.
- 2 In the left pane of the **Protection Settings** dialog box, make sure that a check appears in the check box by **Scheduler**, then select **Scheduler**. The Scheduler Protection Settings page appears on the right.
- 3 Click an entry in the list of things you can schedule. You can select:
 - **Schedule a virus check on all files** on the drives and in the folders you selected in the First Step.
 - **Schedule a virus check on high-risk files** (document files and program files) on the drives and in the folders you selected in the First Step.
 - **Schedule a check on changed files** on the drives and in the folders you selected in the First Step. This check looks at the date of the last virus scan and compares that date with the file date. If the file date is more recent than the scan date, Guard Dog checks the file viruses.
- 4 Click **Next** and follow the instructions on the wizard to set up the schedule.

Tip

If you have any questions about how to use the wizard, click **Help** on any of the wizard screens or press **F1** on your keyboard. Guard Dog displays information specifically designed for the wizard page that is displayed.

As you use the Schedule Wizard, you may want to exclude files and folders from virus checking; for example, you can exclude specific files from large file groups when you know the files are virus free. You can add them to the **Do not check these files and in these folders** in the Virus Sentry Protection Settings page.

Optional Step—Specify what NOT to check during a scheduled virus check

- 1 On the Guard Dog home screen, click **Options** and select **Protection Settings**.
- 2 In the left pane of the **Protection Settings** dialog box, make sure that a check appears in the check box by **Virus Sentry**, then select **Virus Sentry**. The Virus Sentry Protection Settings page appears on the right.
- 3 In the **Do not check these files and these folders**, select what you want to exclude by doing the following:
Click **Add Files** to open the **Add File** dialog box navigate to a specific file.
Click **Add Folders** to open the **Browse for Folder** dialog box and navigate to the folder.

How to check files in one folder

You may need to check only the files in one folder, for example, you have just downloaded something from a Web site that you haven't visited before.

Do this:

- 1 Open My Computer or Windows Explorer.
- 2 Navigate to the folder, and right-click to select it.
- 3 Select **Virus Check** from the pop-up menu.

How to select as-you-work-options in Virus Sentry

When to Check in the Virus Sentry Protection Settings page lets you set up Guard Dog's AntiVirus protection so that you guard against viruses as you actively work on your PC. These checking functions supplement the Virus Check function in CheckUp and the checking options in Scheduler. The as-you-work-options in **When to check** can be combined with CheckUp and Scheduler to complete the protective environment offered by Guard Dog's AntiVirus feature.

How do I change as-you-work AntiVirus protection?

This is a two-step process:

First Step-Select when to check as you work

- 1 On the Guard Dog home screen, click **Options** and select **Protection Settings**.
- 2 In the left pane of the **Protection Settings** dialog box, make sure that a check appears in the check box by **Virus Sentry**, then select **Virus Sentry**. The Virus Sentry Protection Settings page appears on the right.
- 3 In the **When to Check** group box, select or clear the following check boxes:
 - **Program execution**-Scans for viruses when a program starts on your PC.
 - **Email file access**-Scans any e-mail file attachment for viruses when it is opened.
 - **File open**-Scans any file when it is opened.
 - **Move or Rename**-Scans any file when it is moved or renamed.
 - **Floppy drive read**-Select this to scan any floppy disk when it is accessed.
 - **DOS Startup**- Scans DOS for viruses and identify them BEFORE Windows loads each time you start your PC. The Windows operating system still depends on functions provided in an older disk operating system called DOS. Some viruses such as boot sector viruses, partition table viruses, and memory viruses can infect files before Windows loads. Although these virus types may be detected in Windows, most must be cleaned in DOS. For this reason, you should select this setting for more complete virus protection.

Note

You cannot exclude files or programs by adding them to the **Do not check these files or in these folders** list in the Virus Sentry Protection Settings page from **When to check** function.

Second Step-Select how to respond if a virus is found as you work

- 1 On the **Virus Sentry Protection Settings page**, select one of the following from the drop-down list in the **If a virus is found** box:
 - **Automatic Clean**-Removes the virus from the infected file, or failing that prompts you to delete the file.
 - **Automatic Delete**-Deletes the file from your hard drive.
 - **Deny Access**-Blocks you from doing anything with the file, except from deleting it using Windows Explorer or cleaning it by running CheckUp. (When an infected file is opened, the viruses spreads.)
 - **Prompt**-You can decide what to do on a case-by-case basis.

Note

The selection you make in the **If a virus is found** applies to all the selections you make in the **What to check** box except DOS Startup. If a Guard Dog detects a boot sector virus or a virus in memory, Guard Dog displays a message telling you to reboot your PC using the Guard Dog Emergency Disk.

Add Guarded File Wizard page 3

When you add items to the Guarded Files list, this screen displays the file, folder, file group, or drive that you have added. When you are granting access to protected files, this screen displays the file or folder and the program that you have just granted access privileges to. The full path is included for protected files and folders and programs.

To change this information:


 Click **Back** to return to the appropriate wizard screen. Click **Finish** to return to the File Guardian Protection Settings page.

Add Guarded File Wizard page 2

To add a file to the Guarded Files list:

- 1 Type in the path to the file in the text box. For example, if you want to add Spreadsheet.xls in the projects folder on your c drive to the Guarded File list you might type
c:\project\spreadsheet.xls
To avoid typing, click **Browse** to locate the file. The full path appears in the text box automatically.
- 2 To select a file for encryption, select the **Include for file encryption** check box. A lock appears by the file name in the Guarded Files list.
- 3 Click **Next** to display a screen displaying a list of the files you have added.
- 4 To change any information in this screen, click **Back** and make the changes on the appropriate screens. Click **Finish** to return to the File Guardian Protection Settings page.

Tip

To encrypt or decrypt a file in the Guarded File list, right-click the Guard Dog icon  in the system tray and select **Encrypt File Guardian files** or **Decrypt File Guardian files**.

Add Guarded Folder Wizard page 2

To add a folder to the Guarded Files list:

- 1 Type in the path to the folder in the text box. For example, if you want to add all the files in the Project folder to the Guarded Files list, you might type:

c:\project

To avoid typing, click **Browse** to locate the folder. The full path appears in the text box automatically.

- 2 To encrypt all the files in the folder so that the data inside cannot be read, select the **Include for file encryption** check box.
- 3 Click **Next** to display a screen to display a screen displaying a list of the folders you have added.
- 4 To change any information in this screen, click **Back** and make the changes on the appropriate screens. Click **Finish** to return to the File Guardian Protection Settings page.

Add Guarded File Groups Wizard page 2

Guard Dog recognizes files associated with e-mail and financial programs. To avoid adding the files associated with these programs one-at-a-time, Guard Dog treats these files as a group and you can add the group to Guard Files list.

The E-mail file group includes:

- Internet Explorer 4 E-mail
- Internet Explorer 3 E-mail
- Internet Explorer 4 Outlook Express E-mail
- Netscape E-mail
- Communicator E-mail
- Eudora E-mail
- AOL 3 Mail and Password Files

The Financial Files group includes:

- Microsoft Money Financial
- Quicken Financial

To add a File Group to the Guarded Files list:

- 1 Select **File Group** from the list and click **Next** to display a screen containing a list of the groups you have added.
- 2 To change any information in the screen, click **Back** and make the changes on the appropriate screens.
- 3 Click **Finish** to return to the File Guardian Protection Settings page.

Note

You can add these file groups in the Interview portion of the Guard Dog program. See the following topic for more information about restarting the Interview.

[Responding to Interview questions](#)

Add Guarded File Types Wizard page 2

To add File Types to the Guarded Files list:

- 1 Select files types from the list and click **Next**. to display a screen containing a list of the file types you have added.
- 2 To change any information in this screen, click **Back** and make the changes on the appropriate screens. Click **Finish** to return to the File Guardian Protection Settings page.

Tip

To make multiple selection in the list of file types, use SHIFT+CLICK or CONTROL+CLICK.

Add Guarded Files Wizard Drive page 2

To add drives to Guarded Files list:

- 1 Select the drive from the list and click **Next** to display a screen containing displaying a list of the drives you have added.
- 2 To change any information in this screen, click **Back** and make the changes on the appropriate screens. Click **Finish** to return to the File Guardian Protection Settings page.

Tip

To make multiple selection in the list of drives, use SHIFT+CLICK or CONTROL+CLICK.

Add Guarded File Wizard Grant Program Access page 2

To grant program access to the selection you made on the preceding screen:

- 1 Type in the path to the program's executable file in the text box. For example, if File Guardian is guarding your Internet e-mail files you may want to let Microsoft Internet Explorer have access to them. You might type:
c:\Program Files\Internet Explorer\explorer.exe
To avoid typing, click **Browse** to locate the program executable. The full path appears in the text box automatically.
- 2 Click **Next** to display a screen containing a list of the program that you have granted access privileges to.
- 3 To change any information in this screen, click **Back** and make the changes on the appropriate screens. Click **Finish** to return to the File Guardian Protection Settings page.

Add Guarded File Wizard page 1

In this screen, you can either add files—or groups of files—for File Guardian to protect, or you can specify which programs have access to protected files.

To add files to the Guarded Files list:

- 1 Click **Add New Items**.
- 2 Click the arrow beside the drop-down list box to select what to add:
 - **Files**—Add individual files. For example add Spreadsheet.xls to the Guarded Files list. You can tell File Guardian to encrypt files so that the data cannot be read.
 - **Folders**—Add individual folders. For example add My Documents to the Guarded Files list.
 - **File Groups**—Add groups of files. You may not have file groups on your computer.
 - **File Types**—Add file extensions to the Guarded Files list. For example, if you select .doc file extension, File Guardian places .doc in the Guarded Files list and protects all files that have the .doc extension.
 - **Drives**—Add drives to the Guarded Files list. For example, add c:\ to the Guarded Files list and Guard Dog protects all the files and folders on your c drive.

After assigning files, folders, and drives to the Guarded Files list, you can choose which programs are allowed to access these files and folders or you can wait until the file is accessed. Guard Dog will display an alert message from which you can allow a program to access a protected file.

To assign access privileges to the files, folders, and drives in the Guarded Files list:

- 1 Click **Grant Programs Access To**.
- 2 Click the arrow beside the drop-down list box to display a list of the files, folders, and drives you have added to the Guarded Files list and select an entry.
- 3 In the next Add Guarded File Wizard box use **Browse** to find the executable file associated with the program. For example, if you want to let Microsoft Word access any files with a .doc extension, navigate to the folder containing Winword.exe.

Add Financial Information Wizard page 1

Guard Dog will monitor the financial information that you add to Identity Protector. When a program tries to send this information out over the Internet, Guard Dog will alert you based on the options you select on the following wizard screens.

To add financial information to Identity Protector:

- 1 Click the arrow by the **Type** drop-down list box and select one of the following:
 - **VISA**–Select this to enter a Visa credit card number in Identity Protector.
 - **Master Card**–Select this to enter a Master Card credit card number in Identity Protector.
 - **Discover**–Select this to enter a Discover Card credit card number in Identity Protector.
 - **AMEX**–Select this to enter an American Express credit card number in Identity Protector.
 - **Bank Acct**–Select this to enter a bank account number in Identity Protector.
 - **Brokerage**–Select this to enter a brokerage account number in Identity Protector.
 - **Phone Card**–Select this to enter a telephone calling card number in Identity Protector.
 - **Other**–Select this to enter any other type of financial information in Identity Protector.
- 2 Click **Next** to display the next wizard screen.

Add Financial Information VISA page 2

To add a VISA credit card number to Identity Protector:

- 1 Type in a word or phrase to help you identify the card in **Description** box.
- 2 Type the Visa credit card number in the **Visa Card Number** boxes. The cursor jumps automatically from box to box.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Add Financial Information Wizard Master Card page 2

To add a Master Card credit card number to Identity Protector:

- 1 Type in a word or phrase to help you identify the card in **Description** box.
- 2 Type the Master Card credit card number in the **Master Card Number** boxes. The cursor jumps automatically from box to box.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Add Financial Information Discover card page 2

To add a Discover Card credit card number to Identity Protector:

- 1 Type in a word or phrase to help you identify the card in **Description** box.
- 2 Type the Discover Card credit card number in the **Discover Card Number** boxes. The cursor jumps automatically from box to box.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Add Financial Information Wizard AMEX page 2

To add an American Express credit card number:

- 1 Type in a word or phrase to help you identify the card in **Description** box.
- 2 Type the number of the American Express credit card in the **American Express Card Number** box.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Add Financial Information Wizard Bank Account page 2

To add a Bank Account number:

- 1 Type in a word or phrase to help you identify the account in **Description** box.
- 2 Type the number of a bank account in the **Bank Account Number** boxes.
You must click in the box to move the cursor from box to box.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Add Financial Information Wizard Brokerage page 2

To add a brokerage number:

- 1 Type in a word or phrase to help you identify the account in **Description** box.
- 2 Type the number the brokerage account in the **Brokerage Account Number** box.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Add Financial Information Wizard Phone Card page 2

To add a telephone calling card number:

- 1 Type in a word or phrase to help you identify the card in **Description** box.
- 2 Type the number of your telephone calling card in the **Phone Card Number** boxes.
The cursor moves automatically from box to box.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Add Financial Information Wizard Other page 2

To add other critical financial numbers:

- 1 Type in a word or phrase to help you identify the number in **Description** box.
- 2 Type any other critical number in the **Number** box.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Wizard- Financial Info Add Credit Card Info page (don't use)

To add a credit card number to Identity Protector:

- 1 Type the credit card number in the **Credit Card Number** boxes. Use TAB to jump from box to box.
- 2 Type in a word or phrase to help you identify the card.
- 3 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Financial Information Wizard page 3

The information you entered on the Financial Information Wizard screens appears in this box.

To change this information:

 Click **Back** to return to the appropriate wizard page. Click **Finish** to return to the Identity Protector Protection Settings page.

Wizard- Financial Info Types page (don't use)

To add financial information to Identify Protector:

- 1 Click the arrow by the **Type** drop-down list box and choose the type of financial information from the list.
Guard Dog displays wizard page that is applicable to the choice you made in the Type drop-down list box.
For example, if you choose Master Card, Guard Dog displays a page where for your Master Card number. If you choose Phone Card, a page appears where you can enter your calling card number.
- 2 Select one of the following Guard Dog actions:
 - **Allow Always**–Select this if you do not want Guard Dog to alert you when this financial information is sent out over the Internet.
 - **Block Always**–Select this if you do not want this financial information to be sent out over the Internet.
 - **Ask Before Blocking**–Select this if you want to decide on a case-by-case basis. Guard Dog provides an alert message when it detects that this financial information is about to be sent out over the Internet.

Add Identity Information Wizard Address page

To add an address to Identity Protector:

- 1 Complete the screen by typing information in the following boxes for the name that you entered on the Identity Protection Wizard name screen:
 - **Street**–Type the street number and name in this box.
 - **City**–Type the name of the city in this box.
 - **State**–Type the state or province/postal code in this box.
 - **Zip**–Type the Zip code in this box.
 - **Country**–Type the name of the country in this box.
- 2 Click **Next** to display the **More Information** screen.

Add Identify Information Wizard More Information page

To add more information to Identity Protector:

- 1 Click in one of the following boxes and type in the information for the name that you entered on the Identity Protection Wizard name screen:
 - **Social Security Number**
 - **Telephone Number**
 - **E-mail address**
- 2 Select one of the following:
 - **Allow Always**—Guard Dog allows the information entered in this page to be sent out over the Internet.
 - **Block Always**—Guard Dog blocks all attempts to send this information out over the Internet.
 - **Ask Before Blocking**—When Guard Dog detects that this information is about to be sent out over the Internet, Guard Dog provides an alert. The alert message contains options that let you decide how to proceed.

Note

If a Guard Dog password is in use, you must enter the password before information protected by Identity Protector can be sent out.

Add Identity Information Wizard Name page

Guard Dog needs to know who to protect. During the Interview you may have entered your name and now want to edit your information or add someone else's. If more than one person uses this computer, Guard Dog can protect his or her information as well as your own.

To add a name to Identity Protector:

- 1 Type in the name in the appropriate boxes: You can use the TAB key to move from box to box.
 - **First**-Type the first name.
 - **Middle**-Type the middle name.
 - **Last**-Type the last name.
- 2 Click **Next** to display the **Address** page.

Note

You must fill in at least one box on this screen to continue. You are not required to fill in any other boxes in the wizard.

Add Identity Information Wizard Final page

Guard Dog assembles all the information that you entered previously on the wizard screens and displays it on this page for you to verify. If anything is incorrect, just click **Back** to return to the appropriate wizard screen and make any necessary changes. Click **Finish** to return to the Identity Protector Protection Settings page.

Enter password to save Wizard page

To enter a new password and username in Password Manager:




Type information in the following boxes. Use the TAB key to move from box to box.

- **Web Site**—Type URL of the Web site your are connecting to.
- **Username**—Type the username that you use each time you log on the site.
- **Password**—Type the password that you have chosen for this site.


Tip

The information that you enter in this wizard is accessible from the Browser Buddy. To save time and avoid typing errors, you can drag the username and password from Browser Buddy to the appropriate boxes on the Web sites login form.

To display, right-click on the Guard Dog icon  on the system tray and select **Browser Buddy** from the pop-up menu.


Enter password to save Edit page

To add a Password and User ID to the Password Manager

-  Click in the box containing the information you want to change. Use the TAB key to move from box to box.
- **Web Site**—Type URL of the Web site your are connecting to.
 - **Username**—Type the username that you use each time you log on the site.
 - **Password**—Type the password that you have chosen for this site.

Tip

The information that you enter in this wizard is accessible from the Browser Buddy. To save time and avoid typing errors, you can drag the username and password from Browser Buddy to the appropriate boxes on the Web sites login form.

To display, right-click on the Guard Dog icon  on the system tray and select **Browser Buddy** from the pop-up menu.

Add Scheduled Event Wizard Frequency page

To set up a schedule for a selected event:



Click one of the following:

- **Once**—On the next wizard screen use the arrows to select the **Time** and **Date** for Guard Dog to perform the selected event.
- **Hourly**—On the next wizard screen, use the arrows beside the **Minutes after the hour** box to select the time for Guard Dog to perform the selected event. For example if you choose 15, Guard Dog will perform the selected event at 12:15, 1:15, and so forth.
- **Monthly**—On the next wizard screen, use the arrows beside the **Time** box to select the date in the month for Guard Dog to perform the selected event. For example, if you select 5, Guard Dog will perform the selected event on the fifth day of every month.
- **Daily**—On the next wizard screen, use the arrows beside the **Time** box to select the time of day, then select the check boxes by the days of the week for Guard Dog to perform the selected event.
- **Weekly**—On the next wizard screen, use the arrows beside the **Time** box to select the time, then use the arrow by the **Every** list box to select a day of the week for Guard Dog to perform the selected event.
- **Idle**—On the next wizard page, use the arrows to select the **Time** and **Date** for Guard Dog to perform the selected event. This is a good choice if you leave your computer on overnight. You can schedule a time consuming event, such as a thorough virus check when no one is using the computer.
- **Startup**—Guard Dog will perform the scheduled task when you start your computer.

Add Scheduled Event Wizard Once page

Use the arrows to select the **Time** and **Date** for Guard Dog to perform the selected event one time only.

Add Scheduled Event Wizard Hourly page

Use the arrows beside the **Minutes after the hour** box to select the time for Guard Dog to perform the selected event. For example, if you choose 15, Guard Dog will perform the selected event at 12:15, 1:15, and so forth.

Add Scheduled Event Wizard Monthly page

Use the arrows beside the **Time** box to select the date in the month for Guard Dog to perform the selected event. For example, if you select 5, Guard Dog will perform the selected event on the fifth day of every month.

Add Scheduled Event Wizard Daily page

On the next wizard screen, use the arrows by the **Time** box to select the time of day, then select the check boxes by the days of the week for Guard Dog to perform the selected event. For example when you select 1:15 a.m. and Monday and Friday, Guard Dog performs the selected event at 1:15 a.m. every Monday and Friday.

Add Scheduled Event Wizard Weekly page

Use the arrows by the **Time** box to select the time then in the **Every** list box use the arrow to select a day of the week for Guard Dog to perform the selected event. For example, when you select 1:15 a.m. and Monday, Guard Dog performs the selected event at 1:15 a.m. every Monday.

Add Scheduled Event Wizard Idle page

Use the arrows to select the **Time** and **Date** for Guard Dog to perform the selected event. This is a good choice if you leave your computer on overnight. You can schedule a time consuming event, such as a thorough virus check when no one is using the computer.

Add Scheduled Event Wizard Final page

Guard Dog assembles the information that you entered for the selected event and displays it on this screen. If you want to change anything, click **Back** to return to the appropriate wizard screen.

Add Scheduled Event Wizard page 1

To schedule and event:



Click one of the following events in the list then click **Next**:


- **Schedule a virus check on all files**—Checks for viruses in all files on all local drives, including floppy drives, CD-ROM, and removable media drives.
- **Schedule a virus check on high risk files**—Checks for viruses in program and document files on all local drives, including floppy drives, CD-ROM, and removable media drives. This event comes already scheduled to occur when Windows starts.
- **Schedule a virus check on changed files** —Performs a virus check only on files that have been created or modified after the date and time of the last all-file virus check. (It will check all files if they have not been previously checked.)
- **Schedule encryption of my File Guardian files**—Encodes files that are in the Guarded Files list of File Guardian.
- **Schedule decryption of my File Guardian files**—Decodes encrypted file that are in the Guarded Files list of File Guardian.
- **Schedule removal of deleted files on my PC**— Writes over data that remains after files are permanently deleted from your Recycle Bin.
- **Remind to create an Emergency Disk**—When you install Guard Dog, this event will be scheduled to occur every six months.
- **Remind to check for Guard Dog update**—When you install Guard Dog, this event will be scheduled to occur every month.

Guard Dog displays additional wizard pages that let you select a date and time for the selected event.

Virus Sentry Browse for Folder

Because checking for viruses can take a lot of time, you can control how many files Virus Sentry checks by adding folders to the **Do not check these files in these folders** list.

To add folders to the Do not check these files in these folders list:

 Click the folder, then click **OK**.

Tip

This affects not only file-related checks but also the scheduled Quick Virus Check and CheckUp's Virus Check. By default, Guard Dog doesn't check files that are in your Recycle Bin.

Edit Virus Check List Document Files

If you selected Document Files in the **What to Check** box, you can **Add** or **Remove** the types of document files that Virus Sentry checks for viruses.

To add a document type:

- 1 On the Virus Sentry page, select Document Files from the list in the **What to Check** list box, then click **Edit**.
- 2 Click the **Document Files** tab and click **Add**.
- 3 On the next screen select the types of documents that you want Virus Sentry to check and click **OK**.

To remove document types:

- 1 On the Virus Sentry page, select Document Files in the list in the **What to Check** list box then click **Edit**.
- 2 Click the **Document Files** tab, select a document type in the list, and click **Remove**.

Edit Virus Check List

Virus Sentry can check specific program and document types based on what you select in the **What to Check** box on the Virus Sentry Protection Settings page.

To add a program type:

- 1 On the Virus Sentry page, select **Program Files** from the list in the **What to Check** list box, then click **Edit**.
In the **Edit Virus Check List** screen the **Program Files** tab appears by default.
- 2 Click **Add**.
- 3 On the **Add Virus Check List**, select the types of programs and click **OK**.

To add a document type:

- 1 On the Virus Sentry page, select **Document Files** from the list in the **What to Check** list box, then click **Edit**.
- 2 Click the **Document Files** tab to bring it to the front and click **Add**.
- 3 On the **Add Virus Check List**, select the types of document files and click **OK**.

To add a custom file type:

- 1 On the Virus Sentry page, click **Edit**.
- 2 Click **Custom**.
- 3 Type the file extension you want to check and click **OK**.

To reset the default file types to check:

- 1 On the Virus Sentry page, click **Edit**.
- 2 Click **Default**.

To remove a program type:

- 1 On the Virus Sentry page, select **Program Files** in the list in the **What to Check** list box then click **Edit**.
In the **Edit Virus Check List** screen the **Program Files** tab appears by default.
- 2 On the **Program Files** tab, select a program type in the list, and click **Remove**.

To remove a document type:

- 1 On the Virus Sentry page, select **Document Files** from the **What to Check** list box, then click **Edit**.
- 2 Click the **Document Files** tab to bring it to the front, select a document type in the list, then click **Remove**.

Change Guard Dog Password

You can require that anyone using the program enter a password. If you entered a password during the Interview, you can change it using this wizard.

To create a Guard Dog password


- 1 In the **Enter Guard Dog Password** dialog box, type in the password you want to use in the **New Password** box.
- 2 Type the same word again in the **Confirm New Password** box.
- 3 Type a word that Guard Dog can use to remind you of your password in the **Enter a Word** box and click **OK**.

To change the Guard Dog password:

- 1 In the **Change Guard Dog Password** dialog box, type in the password you are using to access Guard Dog in the **Old Password** box.
You can use the TAB key to move from box to box.
- 2 Type the new password in the **New Password** box.
- 3 Type the new password in the **Confirm New Password** box.
- 4 Enter a word to help jog your memory in case you forget the password and click **OK**.
The password takes affect as soon as you create it.

Add Virus Check List

To add file types for Virus Sentry to check:


 Select file types from the list and click **OK** when you are finished to return to the **Edit Virus Check List** screen. Your entry appears at the bottom of the list in the Program Files tab.

Tip

To make multiple selection in the list of file types, use **SHIFT+CLICK** or **CONTROL+CLICK**.

Add Custom Virus Check Extension

To add custom file extensions for Virus Sentry to check:

 Type a three letter file extension in the box and click **OK** to return to the **Edit Virus Check List** screen. Your entry appears at the bottom of the list in the Program Files tab.

Note

A file extension is a part of the name of the file. Windows uses the file extension to determine what kind of information is stored in the file. If it is a document file, Windows uses the file extension to determine which programs are associated with the file. by default, Windows does not display the file extension as part of the file name in My Computer or Windows Explorer.

CyberMedia Emergency Disk Create an Emergency Disk page 1

Guard Dog will write emergency information (files, programs, and Guard Dog settings) to the drive you select from this list. Some things to consider when selecting a drive:


Tip

As a rule you should select a removable media drive, for example your floppy drive. If your emergency information is stored on a network drive, you may not be able to access that drive if you're having problems with your computer.

CyberMedia Emergency Disk Create an Emergency Disk page 2

If you selected your floppy drive on the previous wizard screen, Guard Dog will store emergency information (files, programs, and Guard Dog settings) on three formatted 3 1/2" floppy disks. When the first disk is full, the Emergency Disk Wizard displays a message telling you to insert the second disk.

To start creating an Emergency Disk:

 Insert a disk in your computer's floppy drive and click **Next**.


Tip

You can click **Cancel** to return to the Interview or **Back** to return to the preceding wizard page.


CyberMedia Emergency Disk Create an Emergency Disk page 3

Guard Dog needs a few minutes to copy all the emergency information (files, programs, and Guard Dog settings) to the drive that you have selected. If Guard Dog is copying files to floppy disks, when the first one is full, you will receive a message asking you to insert the second disk.

To continue when Guard Dog completes copying information:

 Click **Next** to continue to the next wizard page.

To stop Guard Dog while it is copying information:


 Click **Cancel**.

When Guard Dog displays a message asking you if you are sure you want to stop, click **Yes** to return to the Interview.

CyberMedia Emergency Disk Create an Emergency Disk page 4

Guard Dog has finished copying emergency information.

To complete the Emergency Disk procedure:

 Click **Finish** to return to the Interview.

