

Contents

Chapter 1: Getting Started	2
Chapter 2: Privacy Control Center	4
Chapter 3: TracksCleaner	11
Chapter 4: Blocking Ads	23
Chapter 5: Stopping Spyware	30
Chapter 6: Protecting Your Data	31
Chapter 7: GhostSurf's Proxy	41
More Help	43

Chapter 1: Getting Started

Introduction

In the physical world, you have a right to privacy. But in the virtual world, everyone from your Internet service provider (ISP), network administrators at work, your boss, other users of your computer, and even web site operators and hackers can watch where you go and what you do.

Welcome to GhostSurf. Now, you're in control. Using the array of tools GhostSurf provides, you can:

- Remove personally-identifying information from web requests, keeping web site operators and advertisers from tracking you online.
- Send your data through Tenebril's high-performance anonymous hubs, hiding your Internet (IP) address and blocking Internet traces back to you.
- Encrypt all the web data to and from your computer, preventing everyone (from your network administrator to your ISP) from seeing what you're doing.
- Block in-page and popup advertisements, to save irritation and save bandwidth.
- Scan your computer for software that could be surreptitiously spying on you, and disable that software when found.
- Scrub unwanted files, and traces of your surfing, with military-grade erasers to keep other users of your computer from discovering your tracks.
- Store important information, personal favorites and passwords in a special encrypted vault so that even if your computer is stolen or used by others, your data is protected.

Now that you have GhostSurf, you have the power to control who sees what, both on your computer directly and through your Internet connection. There's no need to be afraid when you use the Internet, because now you can protect yourself.

Installation

Insert the CD into your CD ROM drive. The installation wizard should begin automatically. If it does not, you will need to manually run the “setup.exe” file on the CD.

Once the installation wizard begins, you will be walked through the process of installing the program. The steps are as follows:

- You will start with a welcome screen. Click ‘Next’ to continue
- You will then be presented with an End User License Agreement (EULA). Read it and click ‘Yes’ to agree and continue. You must agree to the EULA to install and use GhostSurf Platinum.
- Next you will be instructed to choose a folder into which you will install GhostSurf Platinum. Click ‘Next’ to choose the default option, or type in your own path.
- You will now be asked to choose a name for your start menu folder. Click ‘Next’ to choose the default option, or type in your own name.
- Now you will be presented with the options of creating a desktop shortcuts and configuring GhostSurf to automatically make your surfing anonymous. Check the boxes as you wish, and then click ‘Next’ to continue.
- Once you have completed these steps, you will be shown a screen listing the options you have selected. If it is correct, click ‘Next.’ Otherwise, click ‘Back’ to go and fix the problem. The software will now be installed.
- You may need to restart your computer to run GhostSurf Platinum. Once the installation is finished, Setup may ask you to do so.

Once the program is installed, you will need to input your email

address and order number to unlock the product. You will find your order number on the sticker on the CD sleeve.

Chapter 2: Privacy Control Center

Introduction



GhostSurf's Privacy Control Center lets you choose what data will be allowed to reach the Internet, and what data will not. You can also use the Privacy Control Center to send your data through Tenebril's high-performance anonymous hubs, masking your IP address and stopping traces back to your computer. The highest level of privacy also encrypts all your data, so agencies, hackers or your ISP cannot watch your connection to see where you're surfing.

You can set your privacy level by moving the slider (shown above, in the center of the window). The available privacy levels are:

- **Secure** - this is maximum security and anonymity. Outgoing data is modified to remove information that could be used to identify you or reveal some information about the computer you're using. Data is then routed through Tenebril's anonymous hubs to prevent back-

tracing by websites. And everything is encrypted, stopping eavesdropping.

- **Invisible** - this privacy level removes the same personally-identifying information from outgoing data that the "Secure" level does, and routes your data through anonymous hubs to prevent back-tracing. It does not encrypt your data. At this level, a very advanced hacker, a very ambitious ISP, or an agency could listen to your connection to see where you're surfing.
- **Anonymous** - at this level, your personally-identifying information is removed. Data is sent directly to the web sites you're visiting (not sent through anonymous hubs). This may speed up your connection somewhat, but it would allow a malicious web site operator to use your IP address to attack your computer (the web site operator would not know who you are, however). If you visit small websites or websites that are not owned by reputable companies, you may wish to consider using a higher privacy level.
- **Normal** - GhostSurf lets your data go to the Internet directly, just as your web browser sent it. In this sense, you have the same level of privacy that you have if you connect to the Internet without GhostSurf. "Normal" is useful if you're trying to visit a website that requires personal information (like your bank, or your on-line email site).

If you're an advanced user, you can create your own custom privacy levels that are not available by using the slider. To create an advanced privacy level, click the "Advanced..." button in the Privacy Level page. You will now see a set of buttons that will let you define your advanced privacy level. You can choose to block personal information, to route your data anonymously, and to encrypt your data.

You can switch back to the basic privacy levels by clicking the "Simple..." button that appears. When you switch back, the Privacy

Control Center will reset your privacy level to the standard one which most closely matches the advanced one you have created.

Special Site Privacy Levels



You can exclude certain sites from the privacy level you choose on the Privacy Level page of the Privacy Control Center by using this page. Special sites are exempt from the general privacy level. You can use this page to grant a site that requires personal information, like an online banking site or a web-based e-mail site, access to your information even though the general privacy level prevents it.

GhostSurf comes with a number of sites already in the "special sites" list. These sites are popular sites which require personal information, but only for legitimate purposes. For example, Hotmail requires personal information when users log in to check their mail. To allow Hotmail users to use GhostSurf right out of the box, GhostSurf is automatically configured to allow data to reach Hotmail.

To add a site to the "special sites" list, click the "Add" button beneath the list. The window pictured above will appear. You can enter the name of the site in the top box, and choose its privileges below.

Watching Web Traffic



The Traffic page lets you see what information is traveling through GhostSurf. You can also see what modifications GhostSurf makes to the data, and how it anonymizes the data.

The traffic list shows you the requests that your web browser (or other applications that you've configured to use GhostSurf to anonymize their traffic) have made of the Internet. These requests represent the data these applications send to the Internet.

For performance and privacy reasons, GhostSurf does not store a record of your traffic. This means that when you first open the Privacy Control Center, even if you've already been surfing the Internet with GhostSurf, much of your data will not appear in the traffic list. If the traffic list is empty and you have already been using the Internet, don't worry. Try surfing the web while the traffic list is visible -- your requests will appear there.

For each request, you can see what action GhostSurf took (in the "action" column) and what site the request was intended for. To get more information on the request, you can double-click it or you can select it and click the "More info..." button.

You can clear the traffic list by clicking the "Clear" button. This removes all the items from the list. The Privacy Control Center

does not store a record of your traffic, so if you close it and open it again, the list will be cleared.

Who Is This Site?

When you're surfing the web, you have no good indication for who is operating a site you're visiting or even where in the world it is located. Especially for sites that ask for any information (e.g. credit card numbers) that could be harmful if it reaches the wrong hands, it's often useful to know who exactly is in charge of the site. GhostSurf's "Who is" feature can answer that question.

To get information for a site, go to the Traffic page in the Privacy Control Center, click a request associated with that site and then click the "Who is..." button at the bottom of the window. (If you want to get information on a site that does not appear in the list, click on any request; you'll be able to enter another site's name in the "Who Is" window).

The "Who Is" window will appear. It may take a few seconds for the window to appear as GhostSurf looks up the site's records with the Internet database that manages sites. Please be patient. When the records are found, GhostSurf will display them for you as shown.

Managing Add-Ons

GhostSurf can anonymize more than just your web browsing. You can use GhostSurf to anonymize your instant messenger, your IRC chat and NNTP newsreader.

Some add-ons come pre-installed with GhostSurf. To install another add-on, you can double-click the add-on or select it and click on the "Install..." button.

Once you've installed an add-on, you'll usually need to set it up so it can shuttle information properly between your computer and the service the add-on anonymizes. You can set up an add-on by

clicking the "Setup..." button beneath the list when the add-on is selected. For detailed information on setting up each add-on, please refer to the help files in the program itself.

Privacy Control Center Options

The Options page in the Privacy Control Center lets you set some of GhostSurf's more advanced options. These options are primarily intended for advanced users.

The top two buttons, "Start GhostSurf proxy..." and "Automatically direct IE data..." control when GhostSurf starts and what it does when it starts.

For GhostSurf to affect your web data in any way (including anonymizing it, and removing ads), GhostSurf's *proxy* must be running. GhostSurf's proxy receives all incoming and outgoing data, and modifies or blocks it depending on your privacy settings. If the proxy is not running, your data will go directly to the Internet and no privacy protection will be applied. For this reason, you probably want to check the "Start GhostSurf proxy when your computer runs" option. This will keep GhostSurf's proxy running at all times, letting you enjoy the benefits of privacy protection without having to worry about starting GhostSurf manually.

Since your computer and its applications (including Internet Explorer, your instant messenger, and others) must send their data through GhostSurf's proxy instead of directly to the Internet, they must be notified that GhostSurf is running and ready to accept data. GhostSurf is set up to handle this automatically, as long as the "Automatically direct Internet Explorer data through GhostSurf" option is checked. Because no applications will know to send their data through GhostSurf without this option, you should probably leave this option checked.

To prevent personal information from being sent to the Internet, GhostSurf, among other things, directly edits outgoing HTTP requests to remove certain headers. These headers, like "Cookie" and "User-Agent," can be used by websites to track you online and learn what software you're using. By default, GhostSurf blocks the "Cookie" and "User-Agent" headers. You can use the headers list in the Options page to change this, and manage other headers.

To disable a header block (and thus allow that header to pass through to the Internet), you can uncheck its item or delete it from the list. We recommend that you uncheck it; this will take effect immediately and will allow you to re-enable a header block without having to remember what it is called. To delete a header block from the list, select it and click the "Delete" button beneath the list.

To add a header block, click the "Add" button beneath the list. You'll see the window pictured above appear. There you can enter the header's name and choose whether you want the header blocked or allowed through. By default, headers are allowed through -- it is not necessary to explicitly allow a header.

Chapter 3: Tracks Cleaner

Introduction



As you surf the web, your computer keeps detailed records of what you do. Unfortunately, hackers, spying software or simply other users of your computer can use these records to see everything you do. It's nice to have an easy way to clear the records whenever you want.

Tenebril's TracksCleaner securely cleans hundreds of parts of your computer, erasing everything from web surfing records to your clipboard. TracksCleaner also employs advanced deletion technology to prevent erased records from being recovered. And once you set up TracksCleaner, you can run a thorough sweep of your computer with a single click.

Cleaning Your Computer

The "Wipe Now" page lets you choose which parts of your computer TracksCleaner will manage, and then clean them by clicking the "Go" button.

When you first run TracksCleaner, it searches your computer for installed programs and fills the "Wipe Now" list with all the plug-ins that apply to your particular software. You can always add or remove plug-ins from this page by using the Elements page, and you can add folders to clear using the Folders page.

If you want to temporarily change which elements are cleared, you can use the check boxes in the "Wipe Now" list. Only those elements that are checked will be cleaned when you click the "Go" button.

Elements to Wipe



On the "Elements to Wipe" page, you can choose what parts of your computer will be cleaned by TracksCleaner. TracksCleaner offers a library of different plug-ins that manage the parts of your computer, organized into categories. Active plug-ins are green and will appear on the Wipe Now page; blue plug-ins are inactive.

You can activate any of the items in the "Elements to Wipe" page - if you activate one that applies to a program you don't have, it won't hurt your computer. To activate a plug-in, you can select it and click the "Activate" button or simply double-click it. You can also select a category and click the "Activate" button to activate all its plug-ins.

All active plug-ins appear on the "Wipe Now" page and will be applied, unless you uncheck them, to the next cleaning.

You can deactivate a plug-in by selecting it and clicking the "Deactivate" button, or by double-clicking it.

TracksCleaner Plug-In Editor

You can use TracksCleaner's Plug-In Editor to create your own plug-ins or edit the ones that come with TracksCleaner. Creating and editing plug-ins is only intended for advanced users; plug-ins that are improperly designed could delete important information from your computer or otherwise cause significant damage to your work or applications.

Plug-ins are essentially collections of actions TracksCleaner takes when it cleans your computer. Thus, the heart of creating a plug-in is defining the actions it contains. You can use the Add window to add new actions to the plug-in's "Actions" list.

For a detailed explanation of creating new plug-ins, please consult the help documentation inside the program itself.

Wiping Files and Folders

The "Files & Folders to Wipe" page lets you add special files and folders to TracksCleaner's Wipe Now list. These files and folders will be securely cleaned whenever you use TracksCleaner to clean your computer.

To add a file to be cleaned, click the "Add File" button and choose a file from the window that appears. Similarly, you can use the "Add Folder" button to add a folder. Files and folders you add will appear both in the "Files & Folders to Wipe" list and in the "Wipe Now" list.

You can remove a file or folder from the list by clicking the "Remove" button. "Remove" will not delete the file or folder from your computer; it will just remove it from the list.

Clearing Previously Deleted Files



Files you've deleted manually (or potentially with other programs) leave residuals on your computer. These residuals can often be used to reconstruct the deleted files even long after they were deleted. TracksCleaner's "Previously Deleted Files" feature will wipe over these residuals with TracksCleaner's technology, preventing them from being recovered. This will not affect your real files.

To run this feature on your computer's drives, select the ones you want from the list (shown above) and click "Go." When selecting drives, please select drives that are writeable. If you select a CD-RUM, for example, TracksCleaner will not be able to clean it.

While TracksCleaner is working, please close other programs that are running on your computer and avoid creating or deleting files. The sweep TracksCleaner performs is safe and will not harm any of your real files, and even if you do not follow the steps recommended here TracksCleaner will not harm your computer.

You can stop the sweep at any time, but if you stop it before it finishes its work on your disk you may be leaving remnants of previously deleted files behind. To stop a sweep before it finishes, click the "Stop" button.

Protected Elements



It's often important to protect some elements from deletion, like cookies you use to access your favorite sites. This page lets you choose which elements you'd like to protect.

You can add an element to the protected list by clicking the "Add" button. There you can choose to add a cookie, history item or cached page or image to the protected list.

The "Add Protected Element" window lets you browse all the elements on your computer in the box at the top, or enter the information on an element you wish to protect, or both. You can also select more than one element in the browse box.

To make browsing easier, you can use the "Filter" feature. Type in a domain name or part of a name and click the "Filter" button to restrict what is displayed in the browser box.

You can remove an element from the protected list by selecting it and clicking the "Remove" button. Please note that removing an

item from the list does not remove it from your computer -- it simply removes it from protection. You can later re-protect the element if you wish.

Viewing Traces



You can use this page to see what traces of your surfing are on your computer. This feature does not show all traces of your computer use -- rather, it focuses on traces of your web surfing alone. You can use it to manually remove traces if you wish.

From the "View Traces" page, you can see all the cookies, history links and cached elements that Internet Explorer has stored on your computer. To see all the elements of any type, click the "+" button next to the type to expand the view.

If you've used your computer for a long time without cleaning out your traces, you may have very many traces and it may be hard to find any one in particular. You can use the "Filter" feature to help you search for individual traces or sets of traces matching a criterion. Type in a domain name or part of a domain name in the Filter box and click the "Filter" button to display only those items that match your filter. To go back to displaying everything, click the "Clear" button which took the place of the "Filter" button when you clicked it.

Protected elements have a green hue to them. If you've protected any cookies, for example, you may see green-colored ones interspersed in your cookie traces. You can protect an element by selecting it and clicking the "Protect" button, or by double-clicking it. Similarly, you can unprotect an element by clicking the "Protect" button or by double-clicking it.

You can also protect all the elements in a category by selecting the category and clicking "Protect." For example, if you want to protect all the cookies currently on your computer, select the "Cookies" folder and click the "Protect" button.

If you want to manually delete particular elements of your traces, you can select them in the "View Traces" list and click the "Delete" button. You can delete a whole category of traces as well by selecting it and clicking the "Delete" button.

History

The "History" page lets you see what TracksCleaner removed when it was run. You can turn off history-keeping if you wish, and clear the existing history.

To get information on a particular sweep, expand the associated history item by clicking the "+" button next to it. You will see a list of all plug-ins that were applied to the sweep, and all the special files and folders that were cleaned. The "Status" field shows the result of the cleaning.

If you'd like, you can click the "Clear" button to clear all history data. If the "Keep history of wipes" button is not checked, future wipes will not store their history in the list.

Deletion Strength



TracksCleaner provides many options for deleting your data. You can choose from simple methods that effectively protect against recovery to strong government-standard methods that are designed to stop even aggressive hardware recovery systems.

The "Wiping strength level" box lets you choose the method TracksCleaner will use when erasing your data. From weakest to strongest, they are:

- Quick Wipe (normal pass)
- Quick Wipe (random pass)
- Stop Undelete Tools
- NAVSO P-5239-26 (RLL)
- NAVSO P-5239-26 (MFM)
- DOD 5220.22-M
- Schneier's Algorithm
- Super DOD 5220.22-M
- Gutmann's Algorithm

The weaker methods, like Quick Wipe, run faster and are useful if you're deleting a lot of data and aren't critically interested in preventing undeletion. Even the quick methods are strongly effective against undeletion, and will block nearly all undeletion software you can get commercially.

For more information on each of the specific algorithms, please refer to the help files in the program itself.

TracksCleaner offers some additional strength options beneath the "Wiping strength level" box. You can select the "Wipe compressed files" option to treat compressed files specially, managing the data contained therein properly to prevent undeletion. "Wipe slack" gets rid of parts of the disk that are unused but were previously used by a file that TracksCleaner is deleting. "Scramble file and folder properties" cleans out part of the operating system's notes on deleted files. And "scramble alternate data streams" handles special files on some versions of Windows that are stored in multiple areas.

Reporting

You can set up TracksCleaner to notify you by e-mail whenever a wipe completes, and you can also choose whether to be notified before a type of file is erased or when an error occurs.

If you would like to receive reports by e-mail, check the "send email after wipe" box and enter the e-mail address to which you'd like the reports sent. You can choose a format below: either text, HTML or XML. Text e-mails are simple and small, and will work with all e-mail clients. HTML e-mails are fancy webpage-looking e-mails that work with all major e-mail clients. XML is a raw-data format that can be used by system administrators to gather specific information about the wipe.

You can have TracksCleaner ask for confirmation before deleting a file, emptying the recycle bin or before you yourself interrupt an erase. These options are available under the "ask for confirmation

before" section. We recommend that you not select the "normal file" item because it may cause TracksCleaner to ask you often about deleting files as you run a wipe.

You can also have TracksCleaner display status windows when a wipe completes. Choose to have status displayed if an error is encountered, if the wipe completes successfully, or both.

If TracksCleaner encounters errors when it runs your wipe, it will display a window. This window will not display if all plug-ins complete successfully.

This status window displays information on plug-ins that failed to complete successfully. It does not list those plug-ins that completed successfully or those that didn't have any data to delete.

For each plug-in, you can click the "+" button to see specifically what errors occurred.

Scheduler

TracksCleaner can run automatically. This saves you time and energy, and you'll always know that your computer is clean.

You can create a scheduled wipe by choosing its information in the "Create a new scheduled wipe" box and clicking the "Add" button. First, you must choose when the wipe will run. You can choose between when your computer first starts; when all your web browsers are closed; and at a specific time. If you wish to have your wipe run at a specific time, you'll need to choose when and how often it will repeat, if at all.

Once you've defined your schedule, click the "Add" button. The schedule will appear in the list of schedules at the bottom of the "Scheduler" page. You can have as many schedules as you want, but TracksCleaner will prevent you from having multiple copies of the same schedule.

Options



TracksCleaner's options let you run it in stealth mode, hide all your web browsers with a single key press, and manage other hidden elements of TracksCleaner.

If you check the "Run on startup" button, TracksCleaner will start when your computer starts. This is *not* the same as setting a schedule to wipe your computer when it starts; if this box is checked, TracksCleaner will start automatically but it will not wipe your computer (unless you've set a schedule of course).

If you are starting TracksCleaner when your computer starts, you can select the "stealth mode" feature. This will start TracksCleaner silently -- its window and system tray icon will not appear on your screen.

The "boss key" lets you instantly hide all the web browsers on your desktop. These will all come back when you press the boss key again. To activate the boss key, select the boss key box and enter a key in the box next to it. The boss key only applies to Internet Explorer.

You can protect others from using TracksCleaner by selecting the "password protect access" box and entering a password in the window that appears. This will protect you from, for example, having your kids securely delete important files.

TracksCleaner can automatically shut down your web browsers right before it runs a wipe. This is important whenever you're deleting browser data like history or the drop-down bar -- if Internet Explorer is open when you run the wipe, the wipe may not be able to clear out some of this data.

You can select the "disable form suggestions" item to turn off form suggestions in Internet Explorer. This setting will apply even when TracksCleaner is not active.

Finally, you can select the "display system tray tool" item to have TracksCleaner display an icon in your system tray (the lower-right corner of your screen). This is particularly useful if you're running TracksCleaner on startup -- it will allow you quick access to TracksCleaner without forcing its window onto your desktop.

Automatic Updates

You can use TracksCleaner's automatic update feature to get new plug-ins, for free, from Tenebril. New plug-ins will help you remove remnants from new software as it comes out.

To set up automatic updates, click the "check for new plug-ins..." box and enter the frequency with which you'd like TracksCleaner to check for new plug-ins. You can also click the "Check now" button to run a check now.

Chapter 4: Blocking Ads

Introduction



GhostSurf's AdArmor lets you control what you see when you surf the Internet. You can use it to block popup advertisements, advertisements you see directly on web pages, and other common annoyances. Blocking ads not only saves you frustration, but it also speeds up your Internet connection (you have to download less data per page) and it prevents advertising sites from tracking you as you surf.

When you first open the AdArmor window, you'll see three buttons that let you control what is blocked. The first, "Block pop-up ads," will block all pop-up ads if selected (except those from sites you have allowed to display pop-ups, in the Allowed Sites page).

The second, "Block images from advertisers," blocks advertisements directly in web pages. This feature uses the list on the Advertisers page to identify images coming from advertisers and block them. You can use the Advertisers page to allow more ads through, or to block any that you see.

Finally, "Block paid search results" keeps sponsored links from appearing when you search the web with Google, Yahoo, MSN, AllTheWeb, Lycos, AltaVista, AOL and Ask.com. AdArmor constantly updates itself to adapt as search engines change their advertising formats.

The statistics portion of the AdArmor window shows you how many in-page advertisement images AdArmor has blocked, and how many popups AdArmor has blocked.

Advanced Options



The Advanced Options page lets you block more than just popups and search advertisements. You have control over all kinds of webpage annoyances, from text marquees to background music.

You can use the check boxes in the Advanced Options page to block whatever elements you wish. The settings you choose will apply to all websites except those in the Allowed Sites page.

Allowing Advertisements



Although you might want to block advertisements in general, there might be some sites whose popups or ads you might want to let through. The "Allowed Sites" page lets you exempt specific sites from ad-blocking.

Similar to the advertisers list, you can add a site by clicking the "Add" button at the bottom of the list and entering its domain name. When you add a domain to the "Allowed Sites" list, you also choose what privileges you'd like that site to have.

If you later decide you want to revoke a site's privileges, you can uncheck the site in the "Allowed Sites" list or you can delete it entirely by selecting it and clicking the "Delete" button. It is often useful to uncheck the site rather than delete it; that way you can always reinstate the site's privileges by re-checking it in your list.

Advertisers List

The Advertisers page shows all the sites AdArmor recognizes as advertisers, and how many images from each advertiser have been blocked. All the images and pages sent from advertising sites will be blocked. You can use this list to strengthen AdArmor's ad blocking by adding more sites, or weaken it by removing ones that are there.

You can turn off a site (thus allowing images from that site) either by unchecking it or by deleting it. You can delete a site by selecting it and clicking on the "Delete" button. It is probably easiest to simply uncheck (rather than delete) a site, because the result is the same but you still have a record of that site. You can add a site to the list by clicking the "Add" button at the bottom of the list.

Blocking Windows



AdArmor blocks all kinds of popup advertising for you automatically; you can manage popups in the main Options page. The "Window Blocker" feature is different. It blocks actual windows on your desktop, not just webpage windows. You can use it to shut down programs or messages that are annoying. For example, some programs may display a "nag" screen when they first start. You could use Window Blocker to shut down the nag screen automatically, getting you past the nag to the program itself.

Whatever windows you choose to block will be shut down automatically by AdArmor. For this reason, it's very important that you choose windows to block carefully. If you block Microsoft Word, for example, you won't be able to view or edit any Word documents until you turn the window block off.

With that in mind, you can add a window to block by clicking the "Add" button in the "Window Blocker" page. In the "Name" box, you can choose any name you wish to describe this window. The "Text to match" box is the most important element in the window. Here you must enter all or part of the text that appears in the title of the window you wish to block. So if you're blocking Microsoft Word (for example; not recommended), you would type "Microsoft Word". Please make sure you type something specific; if you type "Microsoft", for example, you would block all Microsoft programs.

In the "Microsoft Word" example, you'd need to check the "Match SOME text" box because Word's titles often include other text. For example, if you open a document called "My Recipes", Word's titlebar will say "My Recipes - Microsoft Word". Checking the "Match SOME text" will cause AdArmor to match the "Microsoft Word" text in the title with your block, and close Word. Please note that the "Match SOME text" setting means that AdBlocker will match some of the text in the title with *all* of the text in the "Text to match" box.

Managing Your System

One of the most insidious new advertising methods uses the Windows Messenger Service to pop messages directly onto your screen, even if you're not surfing the web. AdArmor's "System" page lets you turn the Windows Messenger Service off to protect yourself from this. . If you see simple, text-only windows with "Windows Messenger Service" in the title -- the Windows Messenger Service is allowing unwanted advertisements through to your computer.

You can shut down the Windows Messenger Service by clicking the "Stop Windows Messenger Service" button in AdArmor's "System" page. AdArmor will work with your computer to shut down the service and will report the results to you when it's done. You can safely turn off the Windows Messenger Service without

harming your applications. Your instant messaging software will still function correctly.

If you later decide you want to reactivate the Windows Messenger Service, you can always come back to the "System" page. The button will now say "Start Windows Messenger Service;" clicking it will restart the service.

On Windows 95, 98 and ME, the Windows Messenger Service does not run as a standard service (if it runs at all) and cannot be shut down by AdArmor. For that reason, you won't see the "System" page on those operating systems.

Choosing Sounds



You can assign sounds to different events in AdArmor. The "Sounds" page lets you associate sounds with everything from a blocked popup to a blocked sound (ironically).

To add a sound to an event, double-click the event (or select it and click the "Edit" button). A window will appear in which you can enter the file name of a sound. You can also use the window to test the sound you have chosen. The sound file you choose must be in the WAV format.

Once you have associated a sound with an event, that sound will play as long as the check box next to that event is checked. You

can disable a sound by unchecking the box next to its event.

Automatic Updates

Tenebril is constantly adding new advertisers to the advertisers list, to make AdArmor more effective in blocking in-page ads. You can use the Automatic Updates page to have your copy of AdArmor update its advertisers list periodically to keep you protected.

To instruct AdArmor to automatically update your list of advertisers from Tenebril's website, select the "Download the advertisers list" button and enter how often you'd like the update to occur in the box below. When AdArmor updates your advertisers list, it will need to know whether you'd like to automatically block new sites (if you select the "Block this site automatically" button) or if you'd like new sites to be added to the list, but not blocked (the "Add this site to the list, but leave it unchecked").

Chapter 5: Stopping Spyware

What Is Spyware?

Spyware is software that hides on your computer and records the web sites you visit, the keys you press, and almost everything that you do on your computer. You oftentimes download spyware without knowing it. It can collect information about you and secretly send it to the originator using your Internet connection. For example, you can download a game, and spyware can be downloaded at the same time. Usually, the motive is for advertising purposes. However, sometimes the motive is more malicious. Spyware is today's fastest-growing threat to Internet users and is also proving one of the most difficult to solve.

How Can SpyCatcher Help You?

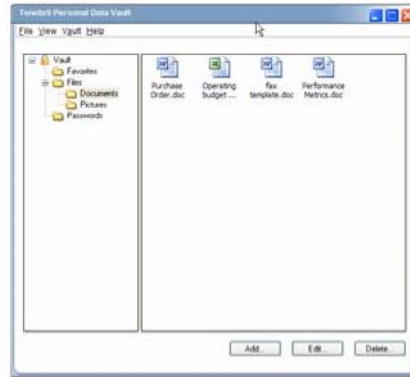
SpyCatcher uses advanced technology to detect and disable thousands of spyware, adware, Trojans and more. SpyCatcher updates itself automatically to provide constant and immediate protection. SpyCatcher is a tool that finds spyware on your computer and allows you to disable it. It is easy to use and keeps your computer safe from adware and malicious software programs. After you set up SpyCatcher to scan your computer regularly, it alerts you whenever it detects spyware or other suspicious programs.

SpyCatcher User Guide

For further information on SpyCatcher please refer to [SpyCatcher Guide](#).

Chapter 6: Protecting Your Data

Introduction



You probably have a lot of data lying around that you want to protect. Passwords are always tough -- if they're on your computer they can get stolen, but if they're on paper they can be lost. Documents sometimes contain sensitive information. Bank records. We generate data all the time, and much of it should be protected.

Tenebril's Personal Data Vault gives you a single, secure place to store your sensitive information. And to protect you from the critical loss of data, Personal Data Vault gives you simple yet powerful backup features. With Personal Data Vault you know your data is protected both from intrusion and from loss.

Your First Vault



When you start Personal Data Vault for the first time you'll need to create your vault. This window will help you.

To create your first vault, enter the name of the vault in the "Vault name" box and enter a password in the "Password" box. Once you've chosen your vault's name and password, click the "Go" button. Your vault will be created and you will see the main Personal Data Vault window. When you next start Personal Data Vault you'll need to log back in to your vault using your password. Your vault's name will be stored in a list so you'll only need to remember your password.

Logging In



This window displays when you start Personal Data Vault. Here you can choose which vault you'd like to view and log into it.

To view your vault, you must first log in. You can choose your vault from the list of vaults and then enter the vault's password. If your vault is not in the list but exists on your computer, you can use the "New" button to add the vault to the list. You can also use the "New" button to create a new, empty vault. You can have as many vaults on your computer as you wish.

Creating a New Vault

This window lets you create a new vault, or tell Personal Data Vault about an existing one.

To create a new vault, enter the name for the vault, the location for its files and its password. By default, the location is "(Default Storage Location)." This will cause Personal Data Vault to store the vault's data in your Application Data folder. This is recommended for all but advanced users.

When you click the "OK" button, your new vault will be created and will appear in the list in the login window.

You can also use this window to import an existing vault. Importing the vault here is not the same as importing files from one vault into another; here you're just telling Personal Data Vault about a vault that already exists but isn't in the login window's list.

You must supply the location of the vault's IDX.PDV file to import it. You can use the "Browse" button to search for the vault's IDX.PDV file.

New Vault Options

You can use this window to choose where you'd like your new vault, and all its encrypted data, to be stored.

By default, Personal Data Vault will create your vault in your "Application Data" folder, which is a hidden folder used by programs to store settings and data. If you would like to choose a different location, you can select the "Use this folder below" option, and enter a folder's path in the box beneath it. You can also use the "Browse" button to choose from a folder on your computer. The folder you enter in the box must already exist on your computer.

Once you've chosen where you'd like your vault to be created, click the "OK" button.

Personal Data Vault Window

The Personal Data Vault window shows you the contents of your vault and lets you perform actions on your vault, like backing it up or importing files. It's easy to add files to your vault -- simply drag them in. You can also add a file by clicking the "Add" button at the bottom of the Personal Data Vault window when viewing a file folder. You can edit files in your vault by double-clicking them. The file will be encrypted and added to your vault; and then the source copy will be securely deleted.

To protect your sensitive files, Personal Data Vault deletes files that are added to your vault by default. You can turn this feature off in the Options window. Please make sure you keep this in mind -- if you add a file to your vault and then lose your password, for example, you won't be able to retrieve your file.

The Personal Data Vault window is similar to Windows Explorer. You can drag files in and out of your vault using your mouse. You can edit files by double-clicking them. And you can navigate through the different folders Personal Data Vault keeps for you using the left-hand pane.

Unlike Windows Explorer, Personal Data Vault organizes your information automatically. If you add a document to your vault, it will automatically fall into the "Documents" folder in the "Files" folder.

Editing and Deleting Files

You can edit files right in your vault, and you can always pull them out of your vault if you wish by dragging them. Files can be deleted as well while within your vault.

Personal Data Vault makes it easy for you to view and edit a file even while it's protected. To view or edit a file, just double-click it in your vault. Personal Data Vault will create a temporary copy of the file outside the vault and then open it with the appropriate program. The temporary copy will persist until your vault is closed. At that time, Personal Data Vault will copy the file back into your vault (preserving any changes you made) and then will securely delete the outside copy.

If you decide that you don't want a file in your vault, you can delete it by selecting the file and clicking the "Delete" button at the bottom of the Personal Data Vault window.

Managing Favorites



Personal Data Vault can store favorites for you. These favorites are accessible only to you.

To add a favorite, click the "Add" button when viewing the Favorites folder (or choose "Add Favorite" from the File menu). The window pictured above will appear. You can enter a friendly name for your favorite (like "My banking site") and the favorite's URL. Or you can choose a favorite from your existing Favorites list by putting a check mark beside it. You can also add a favorite by dragging it directly into Personal Data Vault. If you drop any kind of web link into your vault, it will be stored in your Favorites folder.

You can access a favorite by double-clicking it. This will open your web browser and send it to your favorite's link. You can also drag the favorite outside your Personal Data Vault to create a link.

Managing Passwords

Personal Data Vault can store all your passwords for you. Then you only have to remember one password.

To add a favorite, click the "Add" button when viewing the Passwords folder (or choose "Add Password" from the File menu). The window pictured above will appear. You'll first enter the name for your password record (called the "Location" in the window). You can enter anything you like; this name is just for your convenience.

You can then enter your login name (if any) and your password. Unlike many password entry boxes, in Personal Data Vault your password will be clearly visible. This is by design -- only you will have access to your vault, so your passwords should be easily seen within it.

Backing Up Your Vault

In addition to protecting your sensitive data from being stolen, Personal Data Vault protects it from being lost. You can use Personal Data Vault's backup features to keep your data safe.

To back up your vault, go to the "Vault" menu and choose "Back up." There you can select the drive on which you'd like to make the backup copy. Once you've selected a drive, click the "OK" button. As the backup progresses, you'll watch its progress in the progress bar.

Personal Data Vault can burn CDs and DVDs, so you can choose a drive with an empty CD or DVD in it. You can also choose removable disks like Zip, Jazz, and USB pen drives.

To restore a backup copy of your vault, go to the "Vault" menu and choose "Restore." You will see the "Restore Backup" window, pictured above. There you can choose the place from which your data will be restored. The location of your data on the disk you choose will be automatically determined by Personal Data Vault.

You must enter the password for the vault you are restoring in the password box. Your backup data is still password-protected and encrypted.

When you've chosen your restore settings, click the "OK" button. You will be able to watch your vault's restoration in the progress box.

Options

Personal Data Vault's Options window lets you change how the program behaves on your computer.

If you select the "automatically delete imported files" box, files will be securely deleted from your computer when you add them to your vault. This ensures that only the vault copy of your protected file exists.

Similarly, if you select the "automatically delete vault copy of exported files" box, the vault copy of files will be deleted when you drag those files outside Personal Data Vault. When this setting is used in conjunction with the previously described one, you always have exactly one copy of your data (either inside your vault or outside).

Finally, the "automatically close..." option will close Personal Data Vault automatically after a certain period of inactivity. This protects you from accidentally leaving your vault open when you leave your computer.

Personal Data Vault offers many strong methods for deleting files. These prevent undeletion and recovery tools from regaining your deleted data and will ensure that the only copy of your data is in your vault.

Personal Data Vault can shred your files when they are deleted to

prevent undeletion. You can choose the shredding method in the "Shredding" page of the Options window. The shredding methods offered by Personal Data Vault, sorted from least to most powerful, are:

- Quick Wipe (normal pass)
- Quick Wipe (random pass)
- Stop Undelete Tools
- NAVSO P-5239-26 (RLL)
- NAVSO P-5239-26 (MFM)
- DOD 5220.22-M
- Schneier's Algorithm
- Super DOD 5220.22-M
- Gutmann's Algorithm

For complete information on all of the algorithms, please consult the help documentation in the program itself.

The last tab in the Options window lets you choose whether you'd like to have passwords displayed in your Personal Data Vault or whether you'd like them to be obscured (that is, displayed as "*****"). If you select the "Obscure passwords in the main window" button, passwords will be displayed as "*****" and you'll have to double-click the password to see what it is.

Importing From Other Vaults

You can have more than one vault on your computer, and the Import feature lets you pull data from one vault into another.

To import all the files, passwords and favorites from another vault into the one you currently have open, go to the "Vault" menu and choose "Import." The Import window will appear.

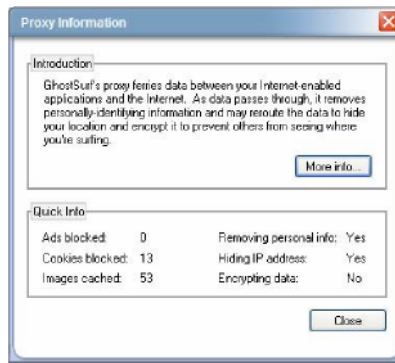
First, you must choose the vault from which to import. Personal Data Vault lists all the vaults that are on your computer in the

"Import from the selected one below" box. You can also import from a vault Personal Data Vault doesn't know about (one from another disk, for example) by selecting the "Import from a special location" box and finding the vault's IDX.PDV file using the "Browse" button. Each vault has an IDX.PDV; you'll need to tell Personal Data Vault where it is for the vault you're trying to import if you choose this option.

Once you have chosen the vault you wish to import, you'll need to enter the password for that vault to gain access to its data. You'll also need to choose whether you'd like to overwrite files you have whose names match those in the imported vault, or rename the imported files so they don't overwrite your current files.

Once you've entered the imported vault's password and chosen your settings, click the "OK" button. The progress bar will show you how the import process is going. When it's done, all the data from the imported vault will be in the vault you're currently viewing.

Chapter 7: GhostSurf's Proxy



GhostSurf's proxy manages privacy protection for the Privacy Control Center. When you're surfing the Internet, the proxy intercepts data before it leaves your computer and filters out personal information. It will also reroute your data through Tenebril's anonymous hubs to prevent websites' tracing you, and will encrypt your data if you are surfing in secure mode. When data comes back from the Internet, the proxy will remove cookies, popups, ads and other nuisances.

When GhostSurf's proxy is running, you'll see GhostSurf's icon in your system tray. As you surf, the icon will blink orange. This indicates that the proxy is receiving data from your web browser and is anonymizing it, or that the proxy has received data from the Internet and is passing it to your browser.

You can move your mouse over the proxy's icon to get statistics on its work, and you can right-click the proxy's icon and choose "Proxy Information" from the menu that appears to get more information on your settings.

If you're surfing in secure mode, you'll also see a lock icon next to the proxy icon. Moving the mouse over the lock will show you some information about the proxy's security strength.

It's important to run the proxy whenever you're using the Internet. When the proxy is running, all your GhostSurf settings (from ad blocking to privacy protection) are enforced. When the proxy is not running, on the other hand, none of your settings apply.

When you install GhostSurf, the installer will ask you if you want to anonymize all the time. If you left this item selected, the proxy was configured to start whenever your computer starts. If not, you can tell the proxy to start automatically by right-clicking its menu in your system tray and choosing "Run on Startup." If this item does not appear, the proxy is already configured to run on startup.

Setting Up GhostSurf With Third-Party Browsers

GhostSurf automatically configures Windows' internal proxy settings to send web traffic through GhostSurf. This means that when GhostSurf is running, all web surfing in Internet Explorer will be anonymized -- there's no need to set up Internet Explorer specially. A number of other web browsers, including the later versions of Firefox, also detect these Windows settings and automatically send their data through GhostSurf.

Some browser lines and some older browsers do not detect the Windows proxy settings, and need to be configured manually to send their data through GhostSurf.

To configure your browser to communicate with GhostSurf rather than to connect directly to the Internet, you must tell it to use GhostSurf as a "proxy" for web traffic. GhostSurf's address on your computer is IP: 127.0.0.1 and Port: 7212. The "127.0.0.1" is the standard way of referring to the local; it is not a real IP address. Port 7212 is the port on which GhostSurf listens for web traffic.

Configuring your browser depends on which browser you're using. Below are step-by-step instructions for Netscape. If you're using a different browser and you can't find its proxy settings, you may wish to refer to its documentation.

INI Settings

INI settings are effectively "hidden" options. They cannot be changed through GhostSurf's Options windows, nor are they intended to be seen by most users. They can be modified by advanced users who need to make GhostSurf perform in a special way. For a complete listing of INI settings, please refer to the help documentation in the program itself.

Electronic Help

The help option on the main menu should be your main source for help, direction, and answering questions. The help pages contain more in-depth coverage of each topic in the manual, and also include a series of articles that explain how and why GhostSurf does what it does.

If you still have a question that cannot be answered by this manual or the help documentation in the program, feel free to contact us by visiting our web site at <http://www.tenebril.com/support>.