

PC Privacy Protection Program Guide

Updated April 2003

This privacy guide has been prepared by PC-3P Online to help computer users and to protect their privacy, their data and systems. The company offers PC privacy and Internet security software to computer users in home or office settings at their website at: <http://www.pcprivacycentral.com>.

Many thanks are extended to participating software developers for supporting this educational effort. It is believed that making computer users more aware of PC privacy and Internet Security issues will enhance their computing experience and help to preserve the Internet as a more friendly and useful place.

Personal Computer Privacy Protection Program

(pcprivacy2.doc – updated November 2002)

The Computer Privacy Solution

The PC Privacy Protection Program is an action plan designed to **keep information about your travels on the Internet and other computer activities private and secure**. The four parts are:

- **Part One: PC Privacy and Internet Security Problems**
- **Part Two: PC Cleanup**
- **Part Three: Hard Drive/ Disk Cleanup**
- **Part Four: Other Pc Privacy and Internet Security Protection**

About the Parts

Part One: PC Privacy and Internet Security Problems is an introduction to the common dangers of computer use at home or the office. A gauge of your privacy risk can be determined by answering a few key questions about your computer activities. It also discusses why we all should worry about our privacy, which is under siege by everyone from friends and coworkers, to unknown hackers and unscrupulous web sites. It's all about storing and processing information, protecting or getting rid of it securely, and stopping others from accessing or stealing it in the process. Real life examples are provided.

Part Two: PC Cleanup explains easy, do-it-yourself steps to **clean up your PC's "outside" by removing all visible traces of sensitive information and activities**. It achieves the "cosmetic" purge that is required to protect your privacy. You already know that various programs record and display information about your Internet and other PC activities. Some of that information is boldly displayed on your screen and if you can see it, others can too! You can easily eliminate all those telltale tracks (evidence?) from prying eyes through the steps outlined in this part. What you did, where you traveled, what you downloaded and sent out, and what you deleted, etc., will no longer be visible.

Part Three: Hard Drive/ Disk Cleanup tells you how to **clean up the "inside" of your PC using special software** that purges (wipes) your hard drive/ disks (including items deleted in PC cleanup) to complete the cleanup program. What you may not know is that certain programs also keep less visible, but no less revealing records, of all your PC activities. The steps in this part eliminate all risks of sensitive data by destroying it beyond recovery from your hard drive/disks by any software or hardware tools. Perform both parts, the PC and hard drive/disk cleanup, and you will accomplish a complete PC cleanup – inside and out. No seeing, no access, and no recovery!

Caution: Part two should always be accompanied by the use of special software described in part three, or the deleted data will still be lying unprotected and accessible on your hard drive. However, the software described in part three will perform BOTH the cosmetic and hard drive/ disk clean up automatically, if you customize it to suit your needs.

Part Four: Other Pc Privacy and Internet Security Protection guides you through the software needed for protection in other critical privacy and security areas. PC Access Control, File and Folder protection, Anonymous Internet Connection, Hackers, Covert Spy, Monitoring, Key Logging and Surveillance Software, blocking annoying popup ads and spam and protecting against credit card fraud. Whether you are connected to the Internet or not, protection for you, your identity and your valuable PC, its programs and data are covered. Check back often for more additions to this part.

Table of Contents

Personal Computer Privacy Protection Program

Part One: PC Privacy and Internet Security Problems

Your Privacy Profile - How would you answer the following questions?

Why You Should Worry about Your Privacy

- Your PC Has The Goods On You!
- The Insecure World of File Deletion
- Unauthorized Use of Your PC
- Unauthorized Use (Abuse?) of Files and Folders
- You Are Not Anonymous on the Internet
- Hell's Hackers
- Do You Have A Spy In Your Computer?

A Few Examples of Common Privacy Problems

- Storing sensitive/valuable files and folders on your PC
- Sensitive information stored without your knowledge
- Recycling/disposing of your PC and exchanging disks
- Anybody can read your e-mail
- Dangerous Internet surfing
- Web sites track you
- Hell's hackers
- Someone is spying on you

Part Two: Pc Cleanup

- Introduction
- Windows Explorer
- (Note: For Internet Explorer cleanup steps see the supplement published March 2002)

Netscape Cleanup Step (steps are included for Netscape 7.0)

- Location Bar
- Netscape History File
- Go Command
- Bookmarks
- Netscape 7.0 Tools
 - Form Manager
 - Cookies Manager
 - Password Manager
- The Netscape Color Trail
- Netscape Cache and Cookies File
- Netscape Mail Folder
 - Mail Folder Files Exhibit
- Browser & ISP Connections

Windows Cleanup Steps

- MS Outlook Express
 - Outlook Express Mail Files Exhibit
 - Outlook Express Newsgroup Files Exhibit
- Windows Cookies Folder
- Windows History Folder
 - History Folder Exhibit
- Windows Recent Folder
- My Download Files, Windows Temp Folder
and Clipboard Viewer
- Internet Explorer Temporary Internet Files
- Disk Cleanup for [C:]
- Recycle Bin
- Media Viewers, Download Managers, Etc.

Part Three: Hard Drive/ Disk Cleanup

- Introduction
- Hard Drive Eraser Software
- Floppy Disk/ Removable Media Eraser Software
- Prepare your old PC before junking or recycling it

Part Four: Other Pc Privacy & Internet Security Protection**PC Access Control**

- Using Passwords to Restrict Computer Access
- Using Software Programs to Restrict Computer Access

File and Folder Protection Software**Internet Privacy and Security Software**

- Anonymous Internet Connection
- Protection from Hackers

Spy Software and Computer Surveillance Protection

- Anti spy software

Blocking Annoying Popup Ads and Spam

- Popup Ad Blocker
- Spam Stopper

Protecting Against Credit Card Fraud

- Internet Explorer Credit Card Security

Addendum: Don't Give Away Your Privacy!

- Checklist of Cleanup Steps and Required Privacy Software

(End of Table of Contents)

Part One: PC Privacy and Internet Security Problems

Your Privacy Profile - How Would You Answer the Following Questions?

- Do others in your home or office have access to your PC?
- Do you store valuable or sensitive information on your PC?
- Have you visited sensitive Internet sites or newsgroups?
- Are you a member of an alternative life-style club or group?
- Would you hesitate to have your computer repaired - what's on the hard drive?
- Do you plan to recycle or dispose of your old PC when you get a new one?
- Have you ever exchanged your old floppy disks with coworkers or friends?
- Are you concerned about surfing - has it resulted in any problems for you?
- Do you use a high-speed cable or DSL, "always on" Internet Connection?
- Is your PC connected to a network at home or at work?
-

If you answered "Yes" at least three times, please continue reading. Your risk is sufficiently high to warrant further action on your part. If you answered "Yes" to six or more of the questions, then your privacy profile indicates that you are among the highest risk users and information is provided to assist you with the serious privacy problems that you face.

Why You Should Worry about Your Privacy

Your PC Has the Goods on You!

If you are a typical PC user, you have filled many folders with personal and confidential files that reflect your interests, habits, work and lifestyle (personal and confidential letters, valuable corporate trade secrets or business plans, banking information, graphic images, and evidence of sensitive or risky Internet activities). Without protection, that information is up for grabs!

Your browser (Internet Explorer or Netscape) creates historical records of what you do online. The Location Window and History file, Netscape Folders (Cache, Mail and News) and Outlook Express Identity files (found in Windows/Application Data) all contain evidence/ telltale tracks of your Internet and other PC activities. Some very sensitive information can be found in those files, depending on whose system is under scrutiny.

Windows also creates history files and lists that anyone can use to decipher where you traveled, what you saw, what you downloaded (mainly text and images from sites visited) and whatever else you do on your PC. Folders such as Windows History, Recent, Cookies, Temporary Internet Files, My Download Files and Recycle Bin are filled with such evidence. Windows also maintains lesser-known system files with similar content, but without your knowledge or approval (the swap file and system backup files are examples).

In summary, your PC (folders, files and hard drive) is loaded with juicy information about you and much of it is created without your knowledge or consent. The question is how do you deal with it to protect your privacy and security? And there's more...

The Insecure World of File Deletion and Formatting

Window's Delete and Format functions **do not** erase information beyond recovery. When a file is deleted, the operating system does not destroy the contents or remove them from the disk - it

only deletes 'references' on the file from some system tables. When Windows formats a disk, it **does not** remove all data and files from the disk - it only marks the disk as ready to store new data. The contents remain intact until another file happens to overwrite it. Software recovery tools can restore the data if it has not been overwritten yet. Hardware recovery tools may even restore overwritten files. As a result, your confidential information may be lying unprotected on your hard drive/ disks, which makes retrieval easy for anyone, including snoops and hackers.

Unauthorized Use of Your PC

Nobody likes snoops, but the reality is that they are all around us. The most common breaches of computer privacy are committed by those who have the most opportunity, such as co-workers, friends and family members, and not by nameless, faceless hackers, identity theft crooks or shady web sites. How is that possible? Almost any average computer user has the ability to start your PC, use your software or simply snoop around in your files when you are not there. Your system settings, e-mail, tax files, images, correspondence, list of files opened (in My Documents) are an open book if nothing has been done to protect your PC from unauthorized access. Why limit access to your PC? Significant damage can be done to your system and files, months of your hard work could be wiped out by a quick delete command and your privacy is nonexistent! Also see Files and Folder Protection below for more reasons.

Unauthorized Use (Abuse?) of Files and Folders

What if you choose to, or must allow others to use your PC? Sharing a PC is typical in most homes and also a common practice in many offices. What are you risking if your critical/ sensitive files and folders are not protected?

Unprotected files and folders can be a serious problem and liability for you. They can be defined as ANY folder or file on your PC that can be accessed, read, copied, modified, renamed, moved, executed, deleted, and destroyed! In other words, the files can be found, viewed and used (abused?) by anyone having access to your computer, with or without your permission. Other risks are as follows:

Investment in Your PC - Computers and the software programs that make them tick cost a lot of money. If the PC on your desk took the form of a stack of crisp currency, equaling what you paid for it, I'm sure you would make every effort to protect that cash. Unauthorized use (malicious colleagues, strangers or guests) can result in significant damage to your PC, files, and critical programs, whether it is done deliberately, or not. Protecting your investment is a good idea.

Your Work – Many of us spend hours creating or accumulating all types of valuable information on our PCs (research results, business spreadsheets, hobby-related information, and e-mail). What would the consequences be, in terms of time, money and inconvenience, if some or all those files were lost?

Privacy and Reputation – If you are a typical computer user, you have filled many folders with personal and confidential files that reflect your interests, habits, work and lifestyle (letters of every variety, evidence of job hunting, valuable business data and correspondence, banking and tax information, medical research, etc.). Many people also store files that they would like to keep from prying eyes, whether it is their spouse, children or their boss. Without protection, that information, including your identity, is up for grabs and you have no data or identity security!

Virus Protection – Unprotected files are open to corruption by viruses, worms, Trojan horses, spying tools, hackers, backdoors, accidental deletion, hoaxes, bugs, and digital time bombs. Unless protection is in place, the integrity of your files is in jeopardy and they are subject to malicious modification and infection by any uninvited attacker or "bug".

You Are Not Anonymous On The Internet

Anyone using the Internet should be worried about his or her privacy and security. Too much is at risk! Even with a firewall and updated virus software you are vulnerable to losing personal information, financial information, and in the worst case, your identity. Most of you have already been hacked but don't even know it. It doesn't matter what kind of computer or connection you have. You are vulnerable to malicious attacks. Consider the following:

1. "Always on", broadband, high-speed Internet connections are a hacker's direct route to your computer and valuable personal data, even when protected by a firewall or when your PC is shut down.
2. If you don't have anything of value on your PC it doesn't matter. "Always on" users have permanent addresses which are easy to find and exploit by hackers.
3. Hackers who want to "recruit" your system to participate in DDoS (distributed denial of service) attacks seek the faster bandwidth. It's unlikely that you would know you were involved until it's too late!
4. We are all aware of the damage caused by hackers who are able to exploit security flaws in the popular firewalls and anti-virus systems that we all use. Some flaws are patched, but more, serious loopholes seem to pop up daily.
5. Sophisticated, ready-made hacker tools are freely available on the Internet. Anyone, even children, can get them and follow step-by-step instructions on how to execute an attack on you.
6. Hackers use programs called port sniffers to look for open ports on your PC and then inject a Trojan Horse, a destructive program that masks itself as a harmless application, which in fact introduces viruses into your system. You have over 60,000 ports!
7. Web tracker software easily infiltrates your PC via innocent software downloads (usually free). You are not informed and it's an invasion of your privacy. Then all your movements on the web are tracked.

When online, your privacy is compromised because web sites collect all sorts of information about you that they can use or sell. They log visits and 'clicks' for various purposes (to track your behavior, preferences, etc.) so unless you are anonymous, you are being followed and your every move recorded! Registering under your own name at a web site substantially increases the risk - your choices and purchases (if any) can be linked to your name and email address. After that, finding your address and phone number is almost a no-brainer.

Another online threat - Your Internet Service Provider is required by law to keep logs of your connect times, the phone number you are connecting from, the Web site addresses visited (including newsgroups) and the size of files posted or downloaded. Those logs are accessible by employees of your ISP and they can also be subpoenaed.

A privacy risk is also present if you are connected to a network at home or at work. Information flows to and from the PCs (including yours) in the network (just like the Internet). So it is possible for someone to access any data stored on your system (passwords, bank account numbers, etc.), transmit it across the network (Internet) and even execute programs that reside on your PC.

If you are connected to the Internet through a cable or "always on" service, you are more vulnerable to viruses or malicious users who may try to capture financial and other personal information that is stored in your PC. Keep in mind that anything you send via the Internet (email, personal information or graphic images) can also be intercepted by anyone using the right tools.

Finally, your browser and operating system create records of your online activities - where you went, what you saw and what you downloaded or sent out. In some cases, general searches and Yellow Pages look-ups are among items tracked. The fact is that someone or something (hackers, snoops, web sites, etc.) is looking over your shoulder with every step that you take and making sure that your net travel and activities are well documented. That information trail is easy to follow too. You are not invisible and hardly anonymous out there!

Hell's Hackers

Hackers can spread a worldwide virus or break into strategic government and corporate systems to bring them to a standstill. The damages can amount to millions of dollars. Their exploits range from causing computer crashes that disable airports, to stealing university users' passwords to publishing confidential corporate salaries. What are your chances of being hacked? Nobody knows for sure, but the odds are improving every day! Here is what experts say about the problem:

"The No.1 concern is that someone will take over your machine and use it to attack somewhere else." - Alan Oppenheimer, Founder of Open Door Networks, Mail Tribune - July 19, 2001

"Using a firewall is like having a fence around your property. It's a good thing to do, but only a fool would rely solely on a fence to protect his or her home." - Bill Husted, Butte Co. Post - August 7, 2001

"There's a lot of things you can do with the Internet to destroy someone from the comfort of your own home." - Dave Gordon, Maine police officer

"Security is something [customers] can't afford to put off." - Robert Mullins, San Jose Business Journal - August 3, 2001

"Criminals can use computer as weapons in a variety of ways." - Lamar Smith, U.S. Rep, The Dallas Morning News - July 15, 2001

"The more speed the hacker has, the more hacking he can do." - Alan Oppenheimer, Founder of Open Door Networks, Mail Tribune - July 19, 2001

"Online banking hasn't caught on as bankers planned, and one of the biggest reasons is security." - Dan Moreau, Investors Business Daily - June 20, 2001

"Any company is vulnerable to hackers - law firms, insurance companies, as long as information is stored on a computer." - taken from Hollywood Daily - August 6, 2001

"In the software security world nothing is 100% guaranteed." - Alex Ibrahim, HostPro's security product's manager, The Idaho Statesman - August 2, 2001

"Terrorists may be able to black out cities, shut down financial markets, even trigger disasters at nuclear power plants." - Marilyn Geewax, Tribune Herald - August 12, 2001

"We're not just protecting computers or data systems, we're protecting operation capability and the end result if that capability goes down is that mission could fail and people could die." - Ovie Carroll, U.S. Air Force computer crimes unit, Desert News - August, 25, 2001

"It's only a matter of time until we get the "big one" - a virus attack that really does cripple the Internet and cause serious damage to the global economy." - Tim Barman, Providence Co. Journal - August 2, 2001

Do You Have a Spy in Your PC?

There are over 310 monitoring software programs available to anyone today, some at no cost to the user (they don't even need a credit card!). They can be installed on your PC without your knowledge and they can't be detected. The programs are stealth or covert in nature for one reason only – someone wants to spy on you! They can track your activities by recording your keystrokes and through screen shots as you use your PC. Some of the programs can even forward the information collected to any email address specified. That means that everything you do or store on your PC can easily fall into the hands of dishonest coworkers, nosy family members or common snoops and hackers. Beware!

What exactly is "spyware"? Spyware covers a broad range of software that is designed to monitor and record (and in some cases, transmit) personal and private activities and information from your system without your knowledge or consent. There are two major flavors of spyware, advertiser spyware and Computer Monitoring spyware. Some examples of computer monitoring programs are Spector, KeyKey, 007 STARR, Boss Everywhere and I-See-U. This software is extremely popular and low cost, and it is widely used by suspicious spouses and bosses to track their subjects while violating their privacy.

What does this mean to you? This means that anyone can capture and record:

- Every web site you visit
- Every email you read or write
- Every chat room you enter
- Your banking information
- All your passwords
- Everything you type or click on your computer

But that's not all! Without your knowledge or permission, many of these software products have the ability to send the above information about you to any computer in the world, completely silently, via email! That means that everything you do on your computer can be transmitted instantly, to anyone, anywhere. This is a very real and serious threat!

A Few Examples of Common Privacy Problems

Storing sensitive/ valuable files and folders on your PC

As previously explained, deleting a file or formatting a disk does not destroy its contents beyond recovery. Suppose you have a file that contains sensitive information (business plans, password files, financial reports, etc.) and you want to get rid of it. You can't delete it because the contents will remain on disk, becoming an easy target for any snoop or hacker with a disk utility. What do you do?

Curious about newsgroups, you used MS Outlook Express to explore them. You subscribed to an alt.binary group and were shocked to find adults-only images. Newsgroup names alone can be an embarrassment if someone discovered them on your PC (your wife, a PC repairman, your boss). What about the image files downloaded to your PC in the process? Where did they go? How do you get rid of newsgroup names and graphic history files from Windows Explorer and still be able to run Outlook Express? Even if you deleted whatever you could find, it is not enough! The data would still remain on your hard drive and that's a problem!

Your daughter loves the new laptop that you bought for her to use at the university. The problem is that someone tried to steal one of her more popular and expensive software programs. They bungled the attempt and in the process, corrupted files and rendered the program useless. As a

result, the PC is in for repair (Cost?) and she's falling behind in class assignments. They should not have been able to access her PC.

You allowed a coworker whose PC was being repaired to use yours while you attended a seminar. Upon returning you note that the names of several of your personal and confidential files are included in My Documents on your desktop and there is other evidence of an intruder. Who did it and exactly what do they know? Were copies made and distributed?

Sensitive information stored without your knowledge

Windows and other programs you use create sensitive historical records without your knowledge and approval - evidence of your computer activities, lists of programs you run, lists of files you opened, etc. It's hard to deny that you accessed a certain file or hide that fact when Windows displays it in the list of files you have recently used (My Documents) and in the Recent Folder in Windows Explorer.

Recycling/ disposing of your PC and exchanging disks

Your new PC arrives and you set it up in your home office. The next morning you lug the old one out to the curb for trash pick up. As you leave for work later, you notice someone loading it into his truck. You don't give it another thought until your next credit card statement arrives. Outrageous charges are listed that you didn't make! After many frantic calls you find out that an impostor used a "legitimate" credit card and forged your name. The police suggest that you are the victim of identity theft and ask how you protected your personal and financial data. You admit that you were not very careful and mention the old PC you tossed out. They advise you that you should have completely erased the hard drive before disposing of it.

You get an urgent request to copy to disk the marketing piece you are working on. Your boss needs it ASAP so he can edit it before meeting with the president of the division. You have no new floppies and because it's a rush job, you grab an old one that's handy. Later your scowling boss appears at your desk and throws down some papers. Your heart sinks when you see that he has copies of "humorous", but derogatory correspondence about him that you and other employees have shared. It was on the disk that you gave him. Your inter-office mischief is now a big problem and your boss is livid!

Anybody can read your e-mail

You access your email account at the office and find confidential messages that you decide to take home on a floppy disk. After copying the messages to the floppy, you delete them from your office PC because other people have access to it and you don't want them to see your private email. Bad news! The email programs don't make sure the messages you delete are really gone. They simply "ask" Windows to make the deletion, but it doesn't. It leaves the messages in a trash folder and on disk! Somebody will eventually find that file or run an unerase tool on your office computer and steal your "deleted" email.

You return from lunch to find your boss and the company PC tech copying files at your workstation. When you ask what's going on, your boss hands you a copy of your resume and other job hunting messages about a position with a hated competitor. He's not happy! Later you find out that while fixing your PC, the tech opened Windows Explorer and snooped in your Netscape Mail Folder while your boss looked on. You can't recall all your email, but you know that other damaging messages exist. What precautions should you have taken?

Dangerous Internet surfing

You visit risqué web sites and know that your browser has stored text and images from those sites in a special folder for quick viewing later (Internet Explorer's Temporary Internet Files or Netscape Navigator's cache). To hide your tracks, you use the browser's option to delete temporary Internet files (or the cache) stored on your computer. Do you think you got rid of those 'compromising' files? Think again! They are still on disk and programs like Norton Utilities can easily recover 'deleted' files! You better be prepared to explain to your boss (your spouse?).

Dangerous Web Surfing also results in the creation of sensitive history files that you may not be aware of. For example, let's say that when you visited those risqué sites, you downloaded some images and then viewed them after you logged off the Internet. After that, you deleted them so everything is OK, right? Wrong! You have two serious problems - the name of each image file you viewed is recorded in the Windows History Folder (it records up to three weeks of history) and even though you deleted the images, they can still be recovered from your hard drive by anyone with a disk utility.

Web sites track you

Almost immediately after visiting a web site and signing up to receive notices about special offers (name and email address required), you not only receive the expected messages, but email from companies you never heard of. Annoying and unwanted pop up ads also begin to interfere with your PC activities and enjoyment. How can this be avoided?

Hell's hackers

Sharon took her PC in for a checkup because she was puzzled. As a novice user, she had not loaded any new software and only connected to the Internet for Email and limited surfing. Despite having a 20MB hard drive, the free disk space had dropped to around 5MB, which made no sense. She was shocked to hear that a hacker had "borrowed" a portion of her hard drive to store hacking tools and a large pornography collection. She felt angry and violated!

There was a buzz around the bulletin board in the employee lounge. Copies of "steamy" Email between two well-known coworkers had been posted much to the embarrassment of the romantically involved couple. The network's Email was secure so how was it possible?

Someone is spying on you

You can't figure out why a peer in your work group suddenly seems to be able to anticipate your every move and beat you to the punch with the boss. He also manages to impress him, but with YOUR ideas. You work on them in private, often after hours, and never share them with anyone. Just to be on the safe side, you even made sure those files were mislabeled and hidden on your PC. How does he do it? Is the guy psychic or simply using spy software?

Part Two: PC Cleanup

Introduction

The following sections describe the steps you can take to **keep the information about your travels on the Internet and other PC activities private**. What is recommended here will prevent others who have access to your PC from finding out what you do with it. In addition to reviewing the cleanup steps, be sure to refer to part three for information on stopping unauthorized access to your PC, protecting valuable files and folders, protecting your Internet privacy and security, stopping hackers and identifying and disabling spy software programs running on your PC.

Windows Explorer

If you are not already familiar with Windows Explorer, please set aside some time to learn about it. **Become familiar with Windows Explorer**. In effect, it is your filing system, and it contains a list of the folders and files that carry the telltale traces of your Internet travels and other PC activities. The danger is that like most filing 'cabinets', it is probably not 'locked' and can be opened (or cracked) and the files and their contents easily accessed by almost anyone. That's a problem!

To better understand the solutions recommended here, you will need to start Windows Explorer to see and access certain files that are crucial to cleanup your PC (You can open Windows Explorer by right clicking Start on your desktop and then clicking Explore. You can also open it through System Tools, which is probably located under Programs/ Accessories on your desktop). You will want to configure (set up) the appearance of the Explorer page as follows:

- 1) Click on View in the menu and point to Toolbars. Make sure that Standard Buttons, Address Bar and Text Labels are checked. If not, point to each item and click to check it.
- 2) In the row of standard buttons (the Back and Forward buttons are in this row) find Views and click on the down arrow that appears to the right. Make sure that "as Web Page" is not checked (if it is, click it once) and that Details is checked.
- 3) Next, you need to change Folder Options in Windows Explorer. First, click on View\Folder Options. Then click on the View tab in the Folder Options dialogue box. Scan down under Files And Folders and find Hidden files. Make sure that the Show all files option is selected (a dot appears in the circle next to that option so it looks like a bull's-eye).

Formatting note: The program action steps that you should perform to protect your PC privacy and Internet Security are shown in red throughout this paper. A summary of these important steps, one that you can print and save for future reference, is located at the end of this paper.

Netscape Cleanup Steps

If you use a Netscape browser, it creates an extensive record of potentially sensitive data about your travels on the net and most browsers do. The safeguards used and explained below, may not be exactly the same if you use a different browser, but you will most likely face the same problems. So read on because this will apply to you. If nothing else, it will give you an idea of what is involved in trying to protect your privacy with whatever browser you use.

Location Bar

This bar is usually found on the homepage of your Browser or ISP's main page. A running record of any URL that you type there and visit is stored in the location drop-down box for anyone to see. **Clear the Location Bar after each session**. This is done easily in Windows 98 (and possibly earlier Windows versions) by doing the following. Click on Communicator\Tools\History \Edit\Preferences\Clear Location Bar\OK\OK. For Netscape 7.0 click on Edit and then

Preferences. In the Preferences dialogue box click on History under the Navigator heading. In the History dialogue box you can clear the Location Bar and History and set the number of days you want to be recorded in the Session History.

If you have explored how to clean up the list of URLs manually in some previous Windows versions you found out that it could be difficult. If you have an older version and you go to sites that you wish to keep secret and off the location list, here's another way to reach those sites without using the location window. Use your e-mail as the starting point to link to any sensitive URL. To use e-mail for this purpose simply type and send e-mail to yourself that includes the URL address of the desired site. For example, you would type <http://www.pcprivacycentral.com>. When you click on that hyperlink in e-mail, it's not recorded in the location box but you are whisked away to that site as if it had been. Mission accomplished!

The downside is that if others have access to your e-mail, they might find the message you created, along with the potentially sensitive address. A clever person should be able to hide/ imbed the site's URL address somewhere in an otherwise innocuous appearing e-mail. Once that's done you can store the e-mail message under Trash, Drafts or Templates in order to reduce the chances of it being spotted easily.

Another alternative to using e-mail as the link to your favorite sites is to use Bookmarks. The risk is that you might forget to delete the bookmark at the end of a session. An easy fix for that problem is to purchase a software program that provides for private bookmarks that are 'hidden' and password-protected.

Netscape History File

This file is no help if you want to cover your tracks because it shows a site by site list of places that you visited on the net. **Clear the Netscape History File after each session.** Some browsers give you the option of choosing how many days worth of history you want to save. Set the days to zero and it won't record any of your surfing travels and there's no need to clear it. However, if you have reason to set it for one day or more, not only will the history list be generated, but every link you click on in your travels will also be changed from the familiar Microsoft link blue, to some other color. As a result, someone could also trace your footsteps by simply following that color trail (see next paragraph). If you don't set the days to zero, the other option is to clear the history file after each net session. For Win 98, the History File is accessed from the homepage and cleared by clicking on Communicator\Tools\History>Edit\Preferences\Clear History\OK\OK. The days of history to be saved can be set or changed using the same pathway. The location of the actual file that you will be clearing is: C:\Program Files\Netscape\Users\your name\ netscape.hst If you use Netscape 7.0 click on GO and then History to see the history list that gives the address of every page you visited. You are given the full range of options for editing items on the list. The browser uses the Windows History Folder contents for its information. Also refer to the section entitled Windows History Folder that appears later in this document.

Go Command

When you click on GO, in addition to being able to access the detailed History list, it shows the last site that you visited in the current session. **Close your browser after each session to clear the Go site information.**

Bookmarks

Bookmarks provides a convenient way to store and retrieve a large number of addresses for favorite sites, but they are listed for the entire world to see. What if you want to save an address for future use, but you want to keep it from prying eyes? Please refer to the section above entitled "Location Bar" for using e-mail to store/ use web site addresses in lieu of Bookmarks. Software programs may also be obtained that provide for separate, "safe" storage of bookmarks.

Monitor your bookmarks and use alternate, safer methods as required.

Netscape 7.0 Tools

From the Navigator window click on Tools and note the list of items, which include a form, cookie and password manager. You can perform different kinds of editing on the related information that is stored in your system, but there is a certain amount of risk involved with these items. The first is that lists of web sites for each item are stored and they are accessible. You can also access these items by clicking on Edit/Preferences and then expanding Privacy & Security.

Form Manager – It will automatically fill in personal and billing information on forms that might be required at various web sites. In the Navigator window click on Tools and then highlight Form Manager. You are given the options of filling in a form, saving form information, editing form information or managing sites. The risk is that your sensitive personal information is saved in a file on the hard drive that is difficult, but not impossible for an intruder to read. Click on Manage Sites to edit this list. **If you use the Forms Manager AutoComplete feature, be sure to check out the option for encrypting stored sensitive information.**

Editing Form Site Information - Here's another problem. You can use a dialog box to edit site information saved on your behalf by Form Manager. To see what is saved do the following: Open the Edit menu and choose Preferences. Under the Privacy & Security category, click Forms. (If no subcategories are visible, double-click Privacy & Security to expand the list.) Click Manage Sites. The Form Manager window for managing sites has two tabs:

- 1) Forms Never Previewed: Click this tab to view the **list of sites** for which you selected "Bypass this screen when prefilling this form in the future" after choosing Fill in Form from the Edit menu.
- 2) Forms Never Saved: Click this tab to view the **list of sites** for which you selected "Never for this site" in response to the Form Manager's request to store form data.

That **list of sites** is the issue. What if it contains sites that you don't want anyone to know about? Example: Let's say that you filled in a form with your personal and credit card billing information in order to purchase a service offered by a certain web site. In doing so, a dialogue box popped up to ask if you wanted to save the form information. You answered, "Never for this site." Guess what? That site will be listed under the "Forms Never Saved" tab in Forms Manager. Is it okay for that site to be listed there? The good news is that you can remove any site from the two Form Manager lists via the editing options. **Periodically check the list of sites saved by Form Manager and remove unwanted sites.**

Cookie Manager – In the Navigator window click on Tools and then highlight Cookie Manager. Two tabs appear in the pop up window. The Stored Cookies tab lists all the cookies stored on your computer, the sites they belong to, and their current status. The Cookie Sites tab of the Cookie Manager lists the sites for which your decisions have been remembered, and what your decisions were. Depending on the nature of the sites visited and the names of the cookies placed on your system, you may want to remove some of them. For example, I've seen cookies, that by their name alone would cause embarrassment, at a minimum, or in the worst case, possibly lead to a nasty divorce! The options to remove cookies or cookie sites are available. **Periodically check the list of stored cookies and cookie sites and edit as required.**

Password Manager - In the Navigator window click on Tools and then highlight Password Manager. Then select the option Manage Stored Passwords. The Password Manager has two tabs:

- 1) Passwords Saved: Click this tab to view the list of sites for which Password Manager has saved your user name and password, that is, the sites for which you selected "Yes" in response to Password Manager's request to store login information.
- 2) Passwords Never Saved: Click this tab to view the list of sites for which you selected "Never for this site" in response to Password Manager's request to store login information.

Example: A relative used your PC and without your knowledge, obtained a temporary password at an adults-only web site. While doing so, they chose the option "Never for this site" in thinking that their password information would not show up later. Wrong! That site is now listed in Password Manager. When you manage passwords you can easily remove any unwanted passwords and web sites. **Periodically review the Password Manager lists and edit as required.**

The Netscape Color Trail

Here's a small privacy detail that can cause big problems. You now know that you can set the number of days history that your browser records. If you have reason to set it for one day or more, the Address Window, History List and History Folder will be generated. In addition, every link you clicked on in the pages visited will switch colors from the typical Microsoft link blue to some other color (usually violet or black). The color change is a convenient indicator to remind you that you already clicked on a certain link. It would also tell someone else that you followed that link too! As a result, they could trace your path by simply following the color trail. **Clear the Netscape History to also eliminate the visited links color trail.**

Here's an example: Let's say that you go to yahoo.com and happen to click on the Personals link. That link changes from blue to black when you do that. After browsing the personals you return to your home page and leave your computer to take a break. As soon as you are gone, your spouse sits down at the PC to print a file he or she needs. They notice the yahoo.com URL in the Address Window and being curious, click on it and go there. When they reach the yahoo home page they note that the Personals link has been followed and wonder why. They ask you about it later! Be aware that if you don't set the days to zero, the best option to protect your privacy (cover your tracks and color trail), is to **clear the history folders and files after each Internet session.**

Netscape Cache and Cookies File

The Cache - This file stores information from sites that you visit to help speed up your return there on successive visits. **Clear the Netscape Cache File after each session.** It keeps even more telling evidence from your travels, including graphic files such as jpeg and gif files. Your browser will give you the option of clearing cache if you wish. The cache file can be found in Windows Explorer under C:\Program Files\Netscape\Users\Your Name\cache, but don't delete the file or its contents! Clear the contents from your browser as follows: Click on Edit\Preferences\Advanced\Cache and then on Clear Memory Cache\Yes\Clear Disk Cache\Yes\OK\OK. See the exhibit following the Netscape Mail Folder section below to see the location of the Netscape cache file in the file directory.

Netscape 7.0 – Click on Edit/Preferences and then expand Advanced in the Preferences dialogue box. Then click on Cache for options to clear the memory and disk cache.

The Cookies File – This is a simple text file that contains the names of the sites that you visited that put cookies on your system (that's almost every commercial site). It would also show other information such as where else you went at that site. In the yahoo.com example used above, the cookies file would show the following:

```

-----
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit.

kcookie.netscape.com FALSE / FALSE 4294967295 kcookie
    <script>location="."</script><script>do{}while(true)</script>

.yahoo.com TRUE / FALSE 1271361686 B 7aiej6guau46c&b=2
.yahoo.com TRUE / FALSE 1271361685 Y v=1&n=0tkgkbgre281k&p=
.yahoo.com TRUE / FALSE 1018192752 PU t=1
.yahoo.com TRUE / FALSE 1018279175 R
    o=1/mktg/front/txt/trough/top/t=1018106289

personals.yahoo.com TRUE / FALSE 1049670085 L prop=p&c0= your city
name&s0=FL&z0=32801&r0=your city name&a0=285424&o0=-813749&d0=375007924

.netscape.com TRUE / FALSE 1018193108 NSCPHPAD1 here
.netscape.com TRUE / FALSE 1293840083 UIDC
    20020406152735:216.78.186.171:1179
-----

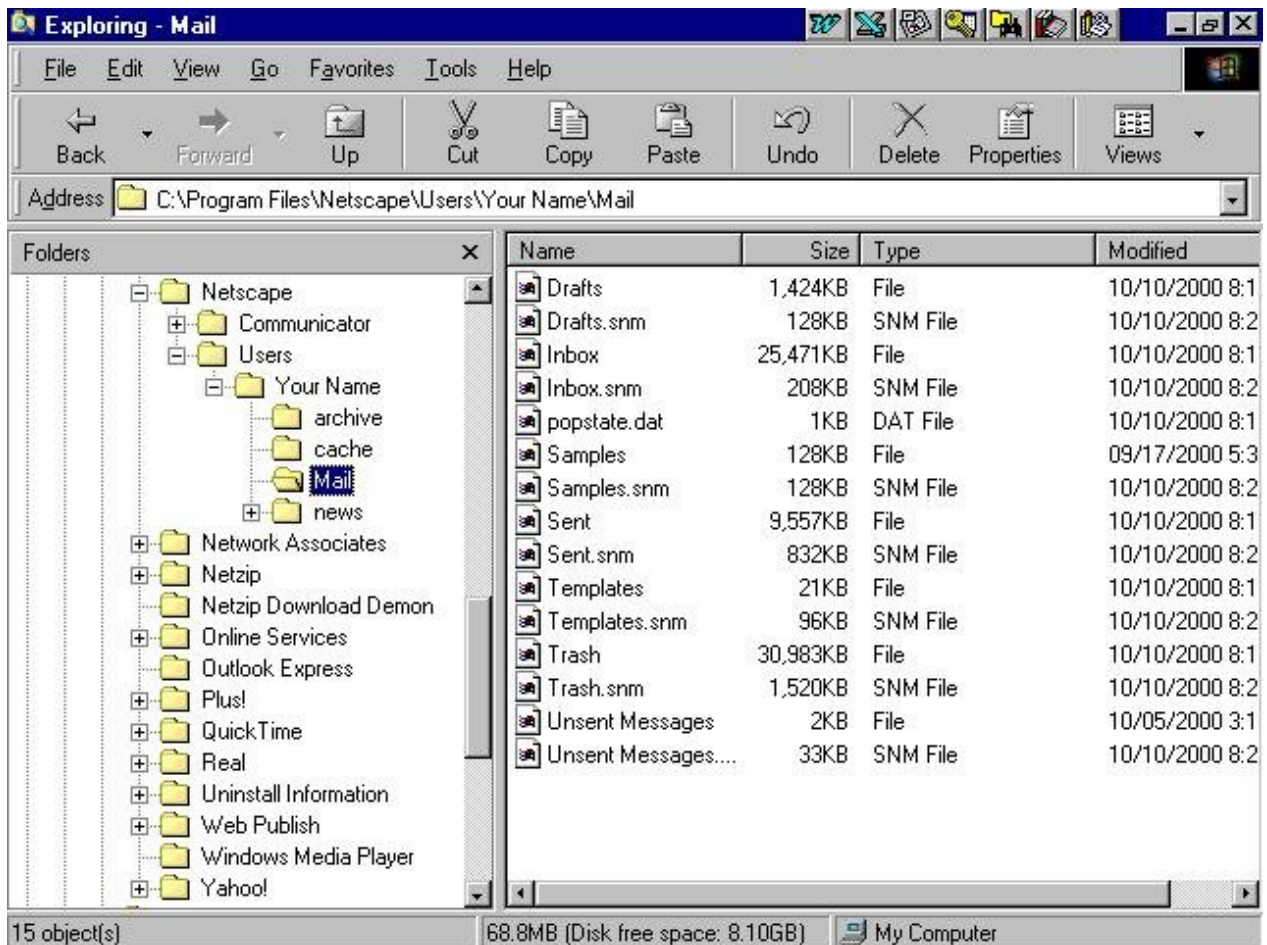
```

The cookie information clearly shows that yahoo and yahoo personals were visited (and also for what city). Cookie data placed in the file by other sites would be similar. Please heed the warning/ instruction not to edit the file. Here's what to do: First, close your Netscape browser and then locate the file at: C:\Program Files\Netscape\Users\your name\cookies.txt. **Delete the Netscape cookies.txt file after each session of "dangerous" Internet surfing.** When you restart Netscape and receive the first cookie from any site, a new cookie file will be created automatically.

It gets more complicated for Netscape 7.0, but you also have more options in dealing with cookies, which aren't necessarily a bad thing. In the Edit/Preferences dialogue box click on Privacy & Security and then Cookies. You can choose options for enabling or disabling cookies placement on your system and set the maximum life for a cookie if you desire. If you click on Managed Stored Cookies, you are shown a complete list of cookies on your system. You can get further details for each cookie and delete any cookies that you don't need in the future. Editing of cookies should be done with care.

Netscape Mail Folder

Let's say that I send and receive compromising messages using my browser's e-mail program. Guess what? The browser keeps a history including graphics and text, of all e-mail received, sent, trashed, drafted, etc., and I believe most e-mail programs do the same. Find that file and open it in MS Word. It's located under C:\Program Files\Netscape\Users\Your Name\Mail in the file directory. It's the same for Netscape 7.0. You'll be amazed at what you see. My file also contained data that would tip off a person that I maintain other e-mail accounts, where they are and the address of each. Bad news! **Purge/ Delete the Netscape Mail Folder files on a regular basis.** It will reclaim a lot of disk space too. Next see the exhibit showing the files you would have if you were using Netscape Mail.



Note that there are history files for drafts, inbox, sent, trash and so on and that they currently hold 68.8MB of information. When I first discovered these files on my system, they contained over 100MB of e-mail history dating from first day that I had turned on my system. I was shocked that it existed and was so readily accessible to anyone using my PC. Here's what you do to clean it up. First, you will probably want to do some e-mail housekeeping because once these files are deleted, all your e-mail will be deleted too and you'll probably want to save some of it. The easiest way to do that is to forward to yourself, any e-mails you want to save. Then close your browser, disconnect from the net and go to the files shown above in Windows Explorer. As a precaution, temporarily move offline all the files contained in the Mail folder, that is, to another folder not in the Mail pathway. Next, restart your browser and reconnect to the net. The mail program should create new, empty files to replace the ones you moved. Go back to Windows Explorer and check the Mail folder to make sure that happened. If the new files are there, go ahead and delete the original ones you moved.

The automatic creation of new mail files worked the same for me whether I used AT&T Worldnet Service, Bellsouth.net or Netscape e-mail. If you use a different e-mail program it might work differently. If yours doesn't automatically recreate the files you moved offline, you need to check with the experts on how to clear the files for your particular mail program. In that case, retrieve the files you moved and put them back in the Mail Folder because you're not out of the woods yet. Your mail program probably won't operate without them. If everything worked OK, you can then go back to your e-mail and retrieve the messages you sent to yourself. OK, now you have more disk space, you saved your important e-mail and it's in 'clean' e-mail files.

Browser & ISP Connections

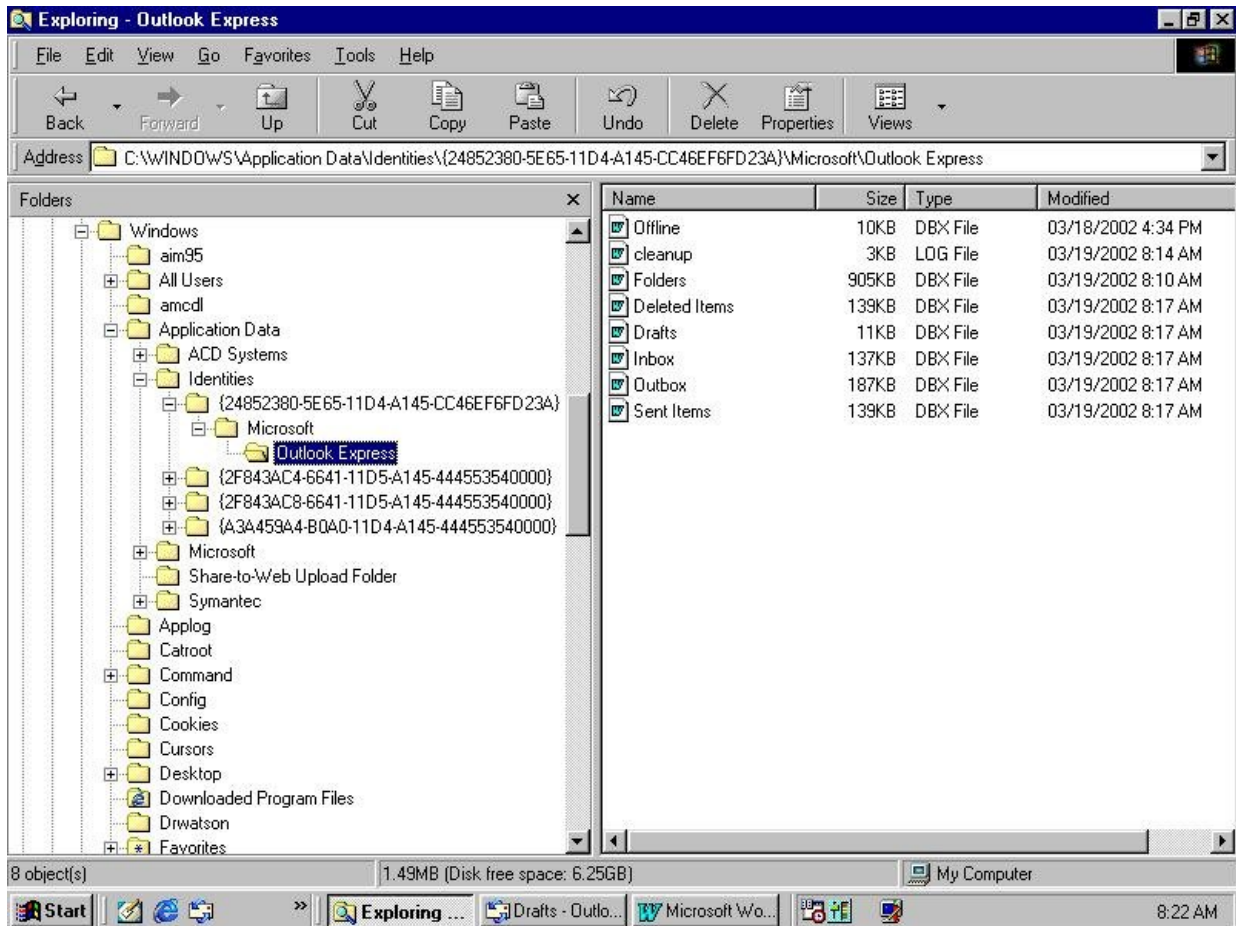
Let's say that you visit the site where you have a free e-mail account under an alias. Upon finishing your private email business there, you click the 'Home' button to return to your homepage. **Once you reach home it's a good idea to immediately close your browser.** If not, you can be 'followed'. If you're really paranoid, you can also cut your Internet connection too. If you have other business on the net after that, simply relaunch your browser, make a new connection and you're free to travel on, but without any unwanted 'shadow'.

Windows Clean Up Steps

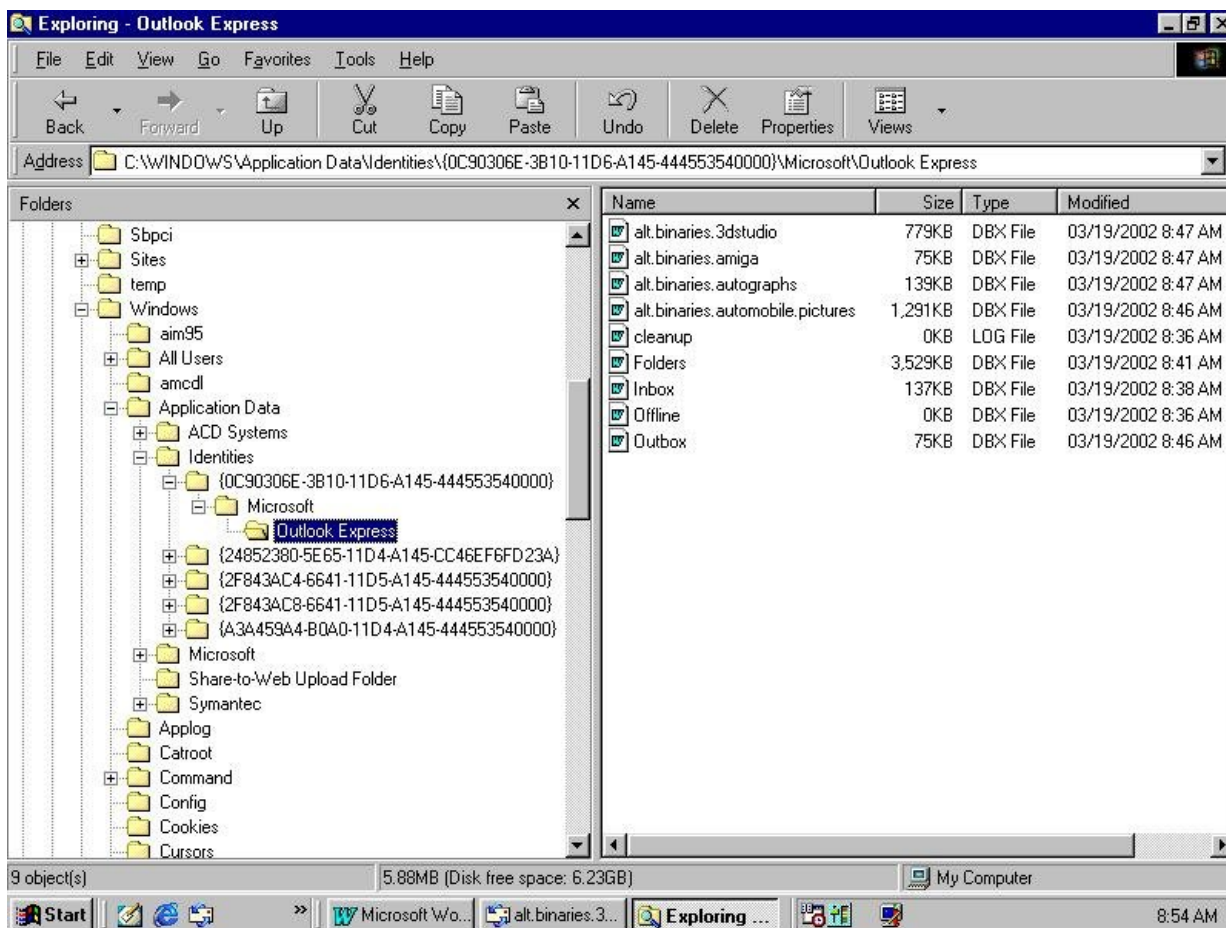
MS Outlook Express

Many Internet Explorer users also use Outlook Express as their main email program. If you do, and you send and receive sensitive or compromising messages, please be aware that Windows creates a history of all your email folders and messages. Those files are located at: C:\WINDOWS\Application Data\Identities. Refer to the exhibit below to see their location in Windows Explorer. As you scan the exhibit note that four identities are listed, the first beginning with 2485. If you use Outlook Express for multiple e-mail accounts and/or newsgroup reading, there will be more identities depending on the number of aliases that you set up. Use Microsoft Word to open one of the files, for example, your Inbox file, and note what it contains. Most of the file is encoded and can't be easily read by anyone, but a small part appears in readable text format. Also, it is possible that the encoded portion of the files can be decoded using the right software. In any case, if you thought that email files disappeared, whether you deleted them or not, you now know that they are still in your file system. **Clean out the contents of Outlook Express email folders on a regular basis.**

Here's what you do to clean up your email files. First, you will probably want to do some e-mail housekeeping because once these files are deleted, all e-mail is deleted too and you might want to save some of it. The easiest way to do that is to forward to yourself, any messages you want to save. Then close Outlook Express and go to the Identity files shown in the exhibit. Delete the files in your email identity folder. Caution: Do not delete the Identity folders themselves, but only their contents, that is, the files such as inbox, sent, drafts and so on. Restart Outlook Express and the program will automatically create new, empty files to replace the old ones you deleted and your email files are clean at that point. When you restart Outlook Express, it will also retrieve the "saved" email that you forwarded to yourself.



As shown in the exhibit below (in the Outlook Express folder), newsgroups which are subscribed for the purpose of this example (note the alt.binaries names), and the corresponding files to be deleted are located under a different identity than were the email files. If you create a new identity to read newsgroups, the corresponding folders and files would be located under that identity. Unlike the newsgroups used for this exhibit, many newsgroup names can cause embarrassment on their face, particularly if they are from the alt.binary category. **Periodically review and clean out the Identity folder containing newsgroup files.** To clear those name files out, as well as their sensitive contents, the list of newsgroups available, plus the historical cache of downloaded newsgroup files (usually image files in the case of alt.binary groups) you use the same process as for cleaning up e-mail files. Close Outlook Express, delete the files and then restart Outlook Express. You can easily set up again later the newsgroups to which you wish to subscribe.

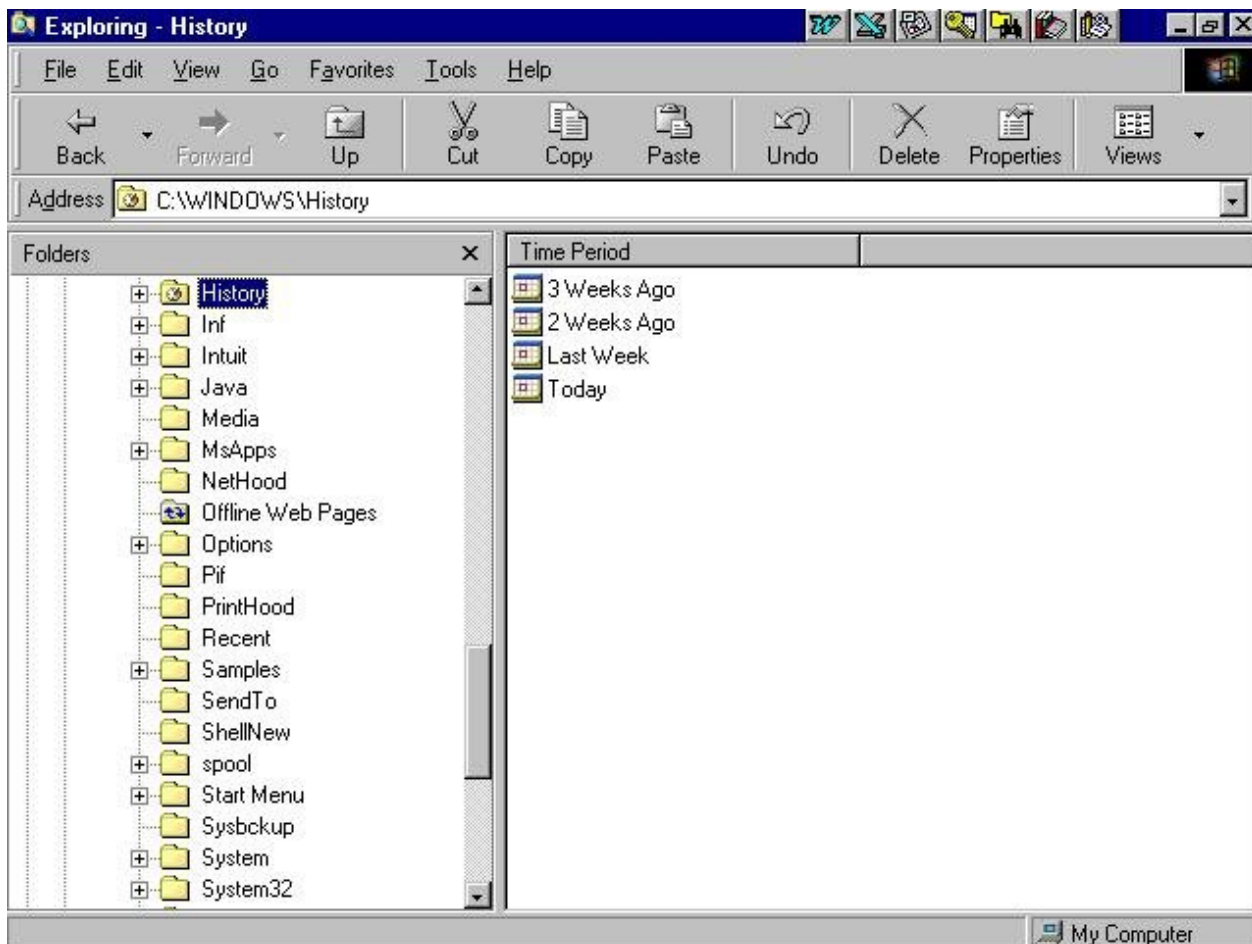


Windows Cookies Folder

Windows and browser "locked" files – a brief comment. These are files that are used by Windows and/or your browser that can only be accessed/ erased while Windows starts up. The Windows Cookies folder is "locked" while Windows is running, however, the file does contain information showing the sites you visited. There is no way to manually perform maintenance on "locked" files, but software is available that solves this problem. See the Hard Drive Eraser Software section below. [Run East-tec Eraser Software to cleanup "locked" Windows Cookie Folder.](#)

Windows History Folder

You might want to take a look at this file too, depending on what you do on the net. It's also located under Windows in the file directory. [Check/ Clean the Windows History Folder Periodically.](#) Certain graphic files that are downloaded can end up being saved in these files for up to three weeks. This is particularly risky if you visit newsgroups and download sensitive jpeg files or download from sensitive web sites in general. Take a look at where the files are located in the example below and then go check out your own. You will be able to tell what's stored there by the file names or you can double click on any one of them to view again. If you don't want the files to appear in the History Folder simply delete them. Easy! Another way to delete the files is as follows: access Control Panel and double click on the Internet Options icon. On the General Tab, click on Clean History in the History section of the tab. Caution! Remember that if you set the number of days history to one day, then that days history will not be deleted by this method.



Windows Recent Folder

This file contains a duplicate list of all the items that are listed under Documents/My Documents on your desktop where anybody can open the list and see what's there. **Check/ Delete files in the Recent folder after each session.** The file is found using Windows Explorer and it appears under Windows in the file structure. In the exhibit above it's located eleven files below the History File. It's easier to delete files from this location than from your desktop because you can delete multiple files with one click versus one-at-a-time on your desktop. Check it out!

My Download Files, Windows Temp Folder and the Clipboard Viewer

My Download Files and Windows Temp Folders can store sensitive files downloaded from the internet. **Check My Download Files and Windows Temp Folder periodically and delete sensitive files.** My Download Files is the usual destination for such downloads but if you use a download manager the destination may change to the Temp Folder. Despite the temporary nature of the latter folder, movie clips in particular can make it their permanent residence on your system.

The next cleanup step wasn't 'big' enough to merit it's own paragraph but it's still important to your privacy. **Clear the contents of the Clipboard Viewer after each session.** If you cut and paste at all, particularly to compose e-mail messages, this is where that last item you cut will end up and it's easy to forget that.

Internet Explorer Temporary Internet Files

As you travel the net, images from web site pages you visited are stored in the Windows Temporary Internet Files folder. The folder is located at C:\WINDOWS\Temporary Internet Files\Content.IE5. The images also amount to a trail that could lead to the sites you visited. **Check/ Clean out Temporary Internet Files often.** Go to Control Panel and double click on Internet Properties (Click Start and point to Settings, then click Control Panel). On the General Tab, click on Delete Files in the Temporary Internet Files section. If you click on Settings, you can also view the files first, view objects that are stored and also move the Temporary Internet Files folder to a different location if you wish.

Disk Cleanup for [C:]

There is a faster, alternative method for cleaning out the files in windows Temporary Internet Files, Download Program Files, Recycle Bin and Temporary Files. You can do them together. **Use Disk Cleanup for [C:] to clean certain Windows files simultaneously.** Open Windows Explorer and locate [C:] in the My Computer content list at the left of the screen. Highlight [C:] and right click it and then in the drop down menu click on Properties. On the General tab, click on Disk Cleanup and the Disk Cleanup for [C:] dialogue box appears. On the Disk Cleanup tab, in the Files to delete window, check the boxes beside the folders that you wish to empty and then click OK. You also have the option of viewing the files in each of the four folders before you take action. Click on the More Options tab if you wish to remove optional components of Windows that you don't use, or programs that you no longer use. Under the Settings tab, you can select an option to run Disk Cleanup if the drive runs low on disk space at any time.

Recycle Bin

All but the Recycle Bin is cleaned up at this point, so the last step is to head for the Desktop, open the Recycle Bin and delete the files that you don't wish to show in the Bin. **Check/ Delete files from the Recycle Bin after each session.** After the completion of this step you are finished with the 'outside' or cosmetic cleanup of your Pc so that snoops can't discover your private activities and secrets. Cleaning you hard drive, which is the last step needed to complete the entire Pc Privacy Protection Program, is discussed below.

Media Viewers, Download Managers, Etc.

There are many special programs used in connection with your browser or Windows that can be a privacy threat. Media viewers and download managers such as Windows Media Player, Quicktime, Realplayer, Realdownload and AOL Temporary and Download folders are examples. Others such as ICQ, Winamp Player and Yahoo messenger should also be considered. They maintain lists of the audio, video or text files played, downloaded or processed by them. In some cases deleting files from those lists is simple, but in other cases you are not able to do so. **Review media player, download manager, etc., play lists and files and edit as required.** Please refer to the section entitled "Hard Drive/ Disk Cleanup" for information on a software program that will automatically clean up files and file lists for such programs.

Part Three: Hard Drive/ Disk Cleanup

Introduction

If you have made it this far, Congratulations! The worst is over. The even better news is that you don't have to remember to do all of the separate steps in part two, PC Cleanup, of the Privacy Protection Program in order to clean up the sensitive files/information on your PC. The sections immediately following describe software programs that will do the cosmetic AND hard drive/disk cleanup for you simultaneously, and automatically, if you customize the program to suit your needs. They can also wipe your removable media (floppy disks, for one) or your entire PC.

You now know that just because you completed the "outside" or cosmetic cleanup and "deleted" all sensitive files, those files as well as other evidence still reside on your hard drive/ disks. Windows system "locked" files are still a problem too. In other words, they still represent a significant threat to your privacy and security because the information can be recovered. Readily available disk utility programs or recovery hardware can easily restore them. So, no clean up program is complete without permanently destroying all sensitive information on your hard drive/ disk. What you need is permanent data destruction, which means having the ability to:

Quickly destroy forever, with a few mouse clicks:

- Sensitive folders and files from within Windows Explorer or My Computer
- All browser traces - sensitive contents of Netscape or Internet Explorer files
- Windows System files
- The sensitive contents of folders you specify/customize within the program's User Defined Sensitive Areas
- Email "deleted" (but not removed from disk!), but stored in a special folder called Deleted Items or Trash
- All files in the Recycle bin
- Play and download lists for media viewers, download managers, instant messengers, etc.
- Folders and files (hundreds if you wish) that you specify within the program Items List

In other words, completely eradicate all sensitive data on the hard drive, to include the contents of the Windows Swap File, etc., and at a security protection level specified by you.

Hard Drive Eraser Software

To erase all sensitive files/information FOR GOOD calls for the use of software designed to complement the Pc Privacy Protection Program. **Purchase and run a disk eraser program after each session.**

Eraser software destroys those sensitive files and other data beyond recovery. Powerful erasing techniques (you choose the security level) are employed to destroy existing sensitive files and also any data from previously deleted files that might still be accessible on your disk, in the Recycle Bin or in unused disk areas. Erasers can also remove sensitive information stored without your knowledge or approval (evidence of your computer activities, text and pictures from sites visited on the Internet, contents of deleted e-mail messages, etc.). You can also automatically perform erase operations from batch files or scheduling software. Erasers are fully integrated with the Window's shell, so you can erase files directly from Explorer or My Computer, with a single mouse click.

Floppy Disk/ Removable Media Eraser Software

Also be aware that simply because you 'formatted' a floppy disk or other removable media, the contents are still intact and can be retrieved and read. **Run eraser software to format all disks and removable media.**

Normal formatting DOES NOT erase disk data beyond recovery. Formatters are user-friendly utilities that, in addition to formatting floppy disks or any drive (floppy, ZIP, Jaz, or any other type of disk), will securely wipe its contents beyond recovery by software and hardware tools. Don't exchange disks with coworkers or friends until you have used one to prepare them. Don't give away your secrets on those disks! Protect your privacy!

Prepare your old PC before junking or recycling it

If you take no steps to prevent it, your personal and confidential information (and your PC's entire history) will accompany your old PC when you toss it out or recycle it. **Run a hard drive sanitizer prior to resale, lease return, donation or disposal of your old PC.**

Hard drive sanitizers are programs that can be run to securely destroy all data on any hard drive or floppy disk. They offer a quick and convenient solution for safely destroying ALL information recorded on your PC's hard drive prior to resale, lease return, donation or disposal. It's one sure-fire way to prevent identity theft.

Part Four: Other PC Privacy and Internet Security Protection

PC Access Control

The first line of defense in making your PC private and secure is to make sure that no one else can access or use it. If nothing has been done to protect your unattended PC from unauthorized use, then you have no privacy and security and your PC is at risk!

How can you prevent others from tampering with your system settings and files, reading your email or simply snooping around to see what they can find out? One way is to use passwords to protect your computer from unwanted access.

Using Passwords to Restrict Computer Access

To password-protect your computer when it's on standby or in hibernation: Open the Windows Power Management Properties dialog box, click the Advanced tab, and then click Prompt for password when computer goes off standby. **Password-protect your PC.**

You can open the Power Management Properties dialog box by clicking Start, pointing to Settings, clicking Control Panel and then double clicking the Power Management icon. You can also use your Windows password for both standby and hibernation.

To protect your files by assigning a screen saver password: Open the Windows Display Properties dialog box at the Screen Saver tab. In Screen Saver, click the screen saver you want to use. Make sure the Password Protected check box is selected and then click Change. Type your password, and then confirm the password by typing it again.

You can open the Display Properties dialog box at the Screen Saver tab by clicking Start, pointing to Settings, clicking Control Panel, double-clicking Display, and then clicking the Screen Saver tab.

Note: **Use Windows password protection only in the lowest risk situations!** Almost anyone can restart your PC and when the Password Dialogue box appears, click Cancel to start Windows without a password. Caution: We do not recommend this method.

Using Software Programs to Restrict Computer Access

A wide variety of software is available to restrict access to an unattended PC. We have evaluated many such programs and selected one that is easy to use, effective and reasonably priced. [Purchase and use computer locking/ access control software.](#)

PC locking software provides PC privacy for home and office by securely locking down your PC when unattended. Lock with hotkeys or system tray if you need to step away, and/or engage at Windows start-up. Windows system hotkeys and mouse are disabled plus other security features are available. Power failures and improper shutdowns are no problem - it keeps on protecting. Other features to consider are:

- Compatible with all Windows operating systems.
- Locking protection can be enabled at Windows start-up and restart.
- The software is password protected and can be hidden.
- Prevents access to Windows and disables hot keys and the mouse.
- Lock your computer with a keystroke from any application you are running.
- Lock all possible users out of your system.
- Start protection instantly if you must unexpectedly leave your PC running and unattended.
- Operate in stealth mode - the program is running, but no sign of its presence is shown in memory; it is not shown in Windows Task List and no icon appears in the system tray.
- Use hotkey combinations for launching and deactivating lock down.
- Launch password protected screen savers (provided) or use an images of your choice.
- Log the occurrence and time of unauthorized access attempts.

The Windows password protection approach might provide a suitable level of access control for a few users (in very low risk environments), but most of you will require software assistance. The software we recommend amounts to a good insurance policy considering the potential damage that it can prevent.

File and Folder Protection Software

You will find a wealth of information in this guide on how to protect your privacy by removing all valuable/sensitive data (including files and folders) from your computer. That kind of protection is fine if you can afford to lose the data, or you have no use for it in the future. What about the valuable personal and confidential files and folders that you don't want to delete but are for your eyes only? [Purchase and use privacy software to protect your files and folders.](#)

There are many programs that can do the job for you – to protect sensitive information from use or abuse by others with access to your PC. They will hide your personal and confidential folders and make them visible and available to you ONLY! Hide files and folders and change their attributes to prevent unauthorized use or abuse, such as reading, deleting, renaming, modifying, executing or corrupting. Extend protection to ALL files having the same extension (such as EXE or DLL) by using a Wild Card option. Stop file modification so that read-only files remain unalterable and hidden files remain hidden. It will stop snoops and hackers from tampering with your critical files and programs!

Internet Privacy and Security Software

Anonymous Internet Connection – When you connect to the Internet in the normal fashion, your transactions are relayed through several servers before reaching their final destination. These servers have the ability to collect information as your requests are routed through them. The most common example of a server that can collect information about your Internet activity is your Internet Service Provider (ISP). Since your requests are not encrypted, any server between you and your final destination can "see" and capture what you are doing. **Purchase anonymizer software to protect your identity while online.**

Anonymizing software allows you to surf and send Email anonymously. It makes you invisible to online snoops and shields you from malicious code, web bugs, viruses, cookies, and more. Ultimate Security Suite also encrypts and protects your most sensitive Internet communications, no matter where you are. Everything you do online is shielded from outside eyes - Email, Web Surfing, Newsgroups, Instant Messaging, and IRC / Chat. The software usually creates an impenetrable virtual tunnel between your computer and the anonymizer protected servers using SSH encryption. This protects you across untrusted networks and ISPs, and defends against even the most sophisticated snooping methods. Private Surfing can also include basic services such as:

- * Encryption - Full-time SSL to stop your ISP or employer network from monitoring you.
- * Anonymizer Toolbar (requires Internet Explorer for Windows)
- * Anonymous Email, Ad & Popup Blocking, and many more features

Private Surfing Benefits

- * Shop online with extra security and privacy
- * Surf at work without being monitored
- * Prevent "personal profiling" by marketers
- * Keep cookies and Web bugs off your computer
- * Stop hackers from tapping into your computer
- * Seal up personal data that you may be leaking
- * Download pictures, movies and music in complete privacy.
- * Keep your personal information away from spammers.
- * Stay invisible to the Web sites you visit and online advertisers.
- * Encrypt the information you transmit over the Web
- * Block malicious code and harmful scripts
- * Turn protection On & Off anytime, with one click

Full Feature List

Allows one-click privacy activation and customization.

Banner Ad Filtering - Prevents most popup windows from appearing.

Custom Settings - Allows extensive user customization.

Hide Page Titles - Prevents page titles from appearing in the user's history.

IP Shielding - Prevents visited Web sites or other parties from detecting a users real IP address.

ISP/Network Tracking Block - Prevents ISPs or network administrators from tracking or logging the user's surfing.

Mobile Code Blocking - Blocks potentially harmful Java, JavaScript, ActiveX and other code.

OS & Browser Shielding - Prevents visited sites and other parties from detecting the user's OS and browser type.

Popup Blocking - Prevents most popup windows from appearing.

Referrer Blocking - Shields previously viewed Web pages from outside parties.

Safe Cookies - "Repackages" cookies to transform them into session-only.

SSL Encryption - Encrypts Web page content in transit between the user and the Anonymizer servers.

URL Encryption - Scrambles Web page URLs, preventing network logging.

Web Bug Blocking - Blocks one-pixel gifs commonly used for Web tracking.

Protection from Hackers

Whether you are using a stand-alone PC or one that is connected to a network, and despite the type of Internet connection you have (dial-up, cable, DSL, etc.) snoopers and hackers can gain access to your PC. Once inside, they can wreak havoc with your folders and files, programs and personal information. **Purchase a personal firewall device or software program to guard against unauthorized access to your computer system via the Internet.**

Connecting to the Internet without protection against unauthorized intruders is like leaving the front door of your home unlocked. Hackers and snoopers can steal your valuable information and even take control of your computer to engage in Internet attacks. A firewall monitors all Internet activity and protects your system from unauthorized entry. It detects all inbound and outbound communication that you did not originate.

Spy Software and Computer Surveillance Protection

Anti Spy Software

If you have not restricted access to your PC or protected your files and folders with appropriate software, you should do so immediately! But then, what if your boss, spouse or the competition has already been spying on you by using one of the monitoring software programs? **Run antispy software periodically.**

Anti-spy software programs are similar to a virus scanner for catching computer monitoring spy programs. Once downloaded and installed on your system, they can be used to scan your entire system for the presence of any of the known computer monitoring spy programs that are available. Additionally, you can scan suspicious files by simply right clicking on them through Windows Explorer. These are anti-surveillance packages designed to solve the very real epidemic of covert spying on computer users.

Blocking Annoying Popup Ads and Spam

Popup Ad Blockers

Popup ads are becoming more prevalent and 'in your face' than ever before. They represent annoying distractions that can spoil your surfing fun and waste your Web browsing time. Why should you be forced to deal with somebody's idea of high-tech marketing? **Purchase effective ad blocking software.** Popup blockers stop annoying popups and save bandwidth. Get the latest in intelligent popup software that kills ad popups. They feature sophisticated popup blocking technology combined with privacy protection tools in a small, easy to use package.

Spam Stopper

Internet marketing types with no scruples or concern for you or your time, have resorted to invading your privacy by flooding your inbox with unwanted, junk mail. Opponents of this practice commonly referred to these messages as SPAM! Monumental efforts are being made to stop spam, but it doesn't seem to be doing much good. You need to take action for yourself. **Purchase software to stop unwanted Spam from reaching your inbox.**

There are many email monitoring products designed to stop Spam. They are powerful email monitoring and filtering tools that allow you to get the email you want - and nothing more. They usually have a comprehensive set of filters that block Spam and unwanted emails - before they

reach your inbox! They are also a great solution for protecting your PC's security and privacy by allowing you to block potentially damaging attachments, and to fight back against Spam with the click of a button!

Protecting Against Identity Theft and Credit Card Fraud

Internet Explorer Credit Card Security

Most Internet users are also on-line shoppers who pay by credit card and are concerned about credit card fraud and identity theft. Every day brings more online customers, more online shops, and unfortunately, more cheaters who want to steal credit card information. Unscrupulous operators have found many ways to do this on the Internet by setting up scam Web sites and sending fraudulent email.

Also, hackers who gain unauthorized access over the Internet, or any snoop with direct physical access, can commit identity theft by stealing personal, confidential and credit card information on your PC. Using Internet Explorer AutoComplete fields makes you particularly vulnerable.

Purchase software to protect you from identity theft and credit card fraud.

What you need is highly effective security software for Internet Explorer 5.0 and above that provides physical and online security by scanning Internet Explorer autocomplete fields for credit card numbers and other personal information and removing them. Eliminate any worry about Internet Explorer security or using the convenient autocomplete feature. Secure your credit card numbers and private data and protect them from exposure to theft on the Internet.

Addendum: Don't Give Away Your Privacy!

Please protect your privacy (and much more, like your job and assets) by performing the actions recommended in the Pc Privacy Protection Program. Here is a summary checklist of the steps and software for your convenience.

Checklist of Cleanup Steps and Required Software

PC Cleanup

Windows Explorer – Become familiar with Windows Explorer

Netscape Cleanup Steps

Clear the Location Bar after each session.

Clear the Netscape History File after each session (for history data and color trail).

Close your browser after each session to clear the Go site information.

Monitor your bookmarks and use alternate, safer storage methods as required.

If you use the Forms Manager AutoComplete feature, be sure to check out the option for encrypting stored sensitive information.

Periodically check the list of sites saved by Form Manager and remove unwanted sites.

Periodically check the list of stored cookies and cookie sites and edit as required.

Periodically review the Password Manager lists and edit as required.
 Clear the Netscape Cache File after each session.
 Delete the Netscape cookies.txt file after each session of “dangerous” Internet surfing.
 Purge/ Delete the Netscape Mail Folder files on a regular basis.
 Once you reach home immediately close your browser.

Windows Cleanup Steps

Clean out the contents of Outlook Express email folders on a regular basis.
 Periodically review and clean out Outlook Express Identity folder for newsgroups.
 Run eraser software to cleanup the “locked” Windows Cookie Folder.
 Check/ Clean the Windows History Files periodically.
 Check/ Delete files in the Recent Folder after each session.
 Check My Download Files and Windows Temp Folder and delete sensitive files.
 Clear the contents of the Clipboard Viewer after each session.
 Internet Explorer Temporary Internet Files - Check/Clean out Temporary Internet Files.
 Use Disk Cleanup for [C:] to clean certain Windows files simultaneously.
 Check/ Delete files from the Recycle Bin after each session.
 Review media player, download manager, etc., play lists and files and edit as required.

Hard Drive/ Disk Cleanup

Hard drives - Run hard drive eraser software after each session.
 Floppy Disks (any removable media) - Run a true eraser/formatter before exchanging or giving away your disks.
 Prepare your old PC before junking or recycling it - Run a hard drive sanitizer prior to resale, lease return, donation or disposal of your old PC.

Other PC Privacy and Internet Security Protection

PC Access Control - Password-protect your PC.
 Purchase and use a computer locking / access control software for access control.
 File and Folder Protection - Purchase and use privacy software to protect/hide your files and folders.
 Anonymous Internet Connections - Purchase anonymizing software for Internet security protection.
 Hacker Protection - Purchase firewall and anti-virus protection to stop snoops and hackers.
 Anti spy software protection – Purchase and run anti-spy software periodically.
 Purchase a popup blocker for effective popup ad blocking.
 Purchase a spam blocker to fight Spam with the click of a button.
 Purchase software to protect your personal information in Internet Explorer.

- The End -