

PC Privacy Protection Program - Internet Explorer Cleanup Supplement

(Version 4.5 Updated April 2003)

Revised April 2007

Internet Explorer Browser Clean Up Steps

Introduction

This supplement to the PC-3P Online privacy guide will help protect your privacy if you use the Internet Explorer browser instead of one of the Netscape versions. The clean up steps described below should be performed along with all other applicable steps in the PC Privacy Protection Program, including the hard drive/ disk cleanup steps, for the best privacy protection results.

Internet Explorer Cleanup

The Internet Explorer browser creates an extensive record of potentially sensitive data (text, images and URLs) about your computer activities and travels on the net. The paragraphs that follow explain how to achieve a browser cleanup to protect your privacy. Other clean up steps (for Windows, Outlook Express, hard drive, floppies, etc.) are also included here because they are closely related to the Internet Explorer privacy problem. The method explained below, might not be exactly the same if you use a different browser, but you will most likely face the same problems, so read on because the information will be useful to you.

Address Window

The Address Window is part of the Internet Explorer tool bar that appears at the top of your screen. A running record of web site addresses (URLs) that you enter there and visit is stored in the address drop-down box for your convenience if you want to revisit those sites at a later time. The problem is that anyone can access the addresses to see where you have been and that's a privacy problem. **Clear the Address Window after each session.** To do so click on Tools and then Internet Options and the Internet Options dialogue box will appear. Under the General tab locate the History section and click on Clear History and then click OK.

Please note that the number of day's history of URLs that are recorded by your browser can also be set or changed in that same History section. You can do so by changing the number indicated in the Days to keep pages in history counter. Caution: Unless you set the counter to zero, URLs will continue to be recorded.

If you have explored how to delete the list of URLs manually for some previous Windows versions you found out that it could be difficult. No matter what version you use, if you go to sites that you wish to keep secret (off the address list), here's another way to reach them to prevent the address from being recorded. 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 the URL in the following format: <http://www.pcprivacycentral.com>. When you click on that hyperlink in e-mail, Internet Explorer takes you to that site, but does not record the URL.

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 Deleted Items or Drafts, for example, or wherever you think they will be harder to spot.

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.

Favorites

By using the Favorites/Add to Favorites commands in the Internet Explorer tool bar, you can add the addresses of your favorite web sites to your Favorites list for greater ease in visiting there again. This is convenient for you and also for anyone else who wants to find out what sites you visited. **Check the Favorites list frequently and delete items that should not appear there.** There are two ways to delete items from your Favorites list. You can right click on each item listed and in the pop up menu that appears, point to and click on Delete. That method allows you to delete your favorites one at a time. Here's a quicker way to handle the deletion if you have a number of items. Open Windows Explorer, find Windows and expand it. Scroll down to Favorites and click on it to see the various folders and web sites that make up your Favorites list. You can highlight each item you wish to delete by left clicking on the first item to highlight it. Then while holding down the CTRL key, left click on the rest of the items to be deleted. When you are done, point to any of the highlighted files and right click. In the menu that appears, point to and click on Delete. This action simultaneously deletes all the files you highlighted and you are done. Remember that the deleted items are in the Recycle Bin, so you are not finished until they are deleted there also.

Internet Explorer History Button, History List and History Folder

The Internet Explorer History records are no help in covering your Internet tracks because they show a site by site list of addresses that you have visited. Click on the History button in the tool bar at the top of your screen to open the History List. The list shows the sites you visited, and if you have not adjusted the number of days of history to be recorded, it could show up to three weeks of your travels that anyone can see. **Clear Internet Explorer History after each session.** This is accomplished in the same way that you cleared the Address Window. Click on Tools and then Internet Options and the Internet Options dialogue box appears. Under the General tab locate the History section and click on Clear History and then OK.

Windows History Folder

The files displayed in Internet Explorer History are a mirror image of files found in the Windows History folder. Please note that you can also delete these files from Windows Explorer. **Clear (delete) all files in the Windows/History/Today folders after each session.** Do the following to clear out the Windows History Folder: Open Windows Explorer (right click on Start on your desktop and then click Explore), find the Windows item and expand it, then scroll down to the History folder and click on it. Then click on Today and then the subfolder under Today. The addresses you have visited will be displayed in the right portion of the screen and they should be deleted. To delete the files quickly, left click on the first file in the list to highlight it. While holding down the Shift key, left click on the last file in the list. All files to be deleted should be highlighted at that point. Then point to any of the highlighted files, right click and then point to and left click on Delete in the drop down menu.

The Windows 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 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 IE History to eliminate the visited links color trails.** 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.**

Windows Cookies Folder

Windows and Internet Explorer "locked" files – a brief comment. These are files that are used by Windows and/or Internet Explorer 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.

Internet Explorer Temporary Internet Files

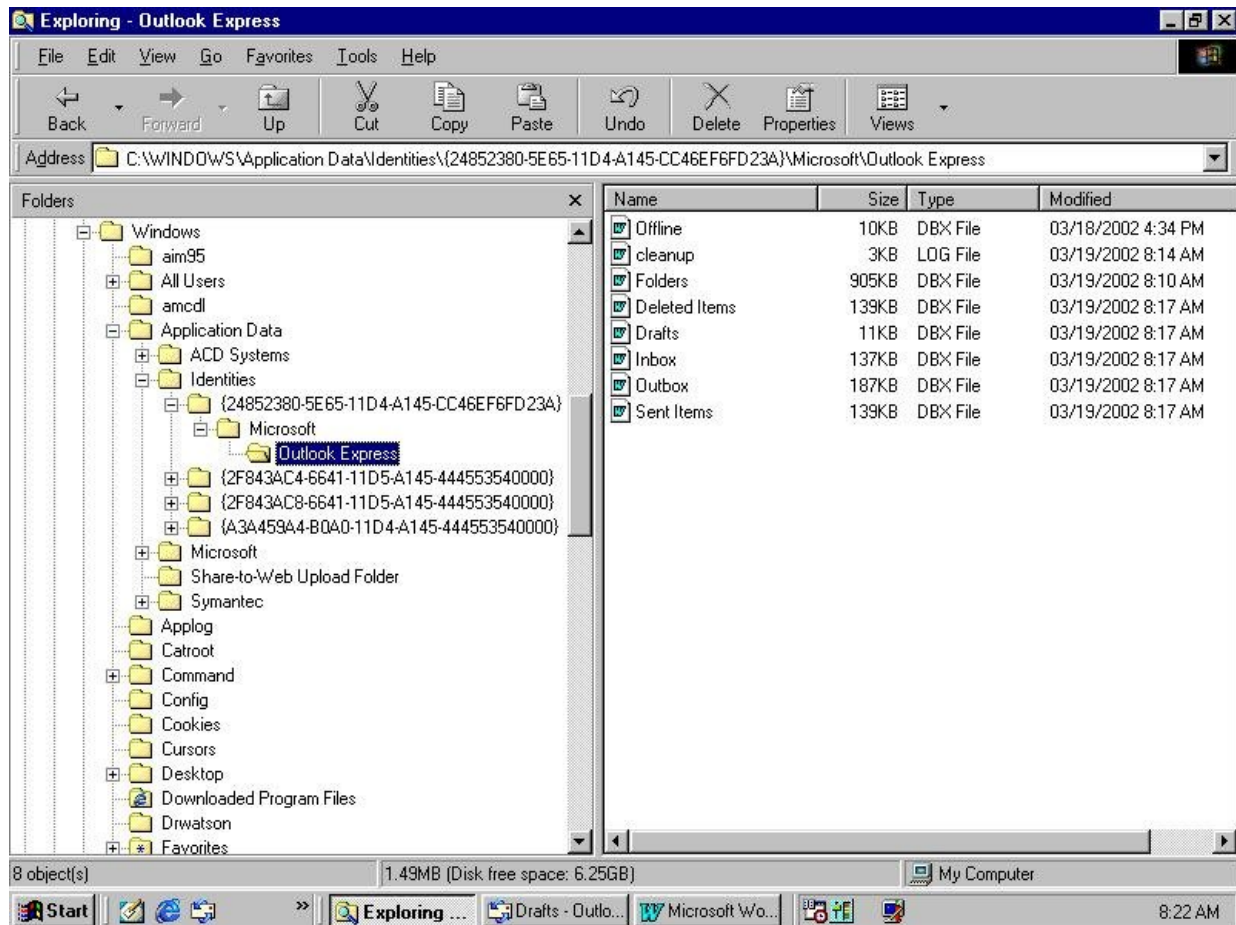
As you surf the net, data from web pages you visited is stored in the Windows Temporary Internet Files folder. The folder is located at C:\WINDOWS\Temporary Internet Files\Content.IE5. Those files amount to a trail that could lead back to the sites you visited. **Check and clean out Temporary Internet Files often.** Click on Tools and then Internet Options to open the Internet Options dialog box. Under the General tab locate the Temporary Internet Files section. If you click on Settings first, you can review the files to be deleted, view objects that are stored and also move the Temporary Internet Files folder to a different location if you wish. Then click on Delete Files... and click OK in the Delete Files confirmation box. Note that you are also given the option of deleting all offline content that you have stored on your computer. Checking that box will also delete, for example, any web pages, that you saved for offline viewing, and other content placed in the temporary file by web sites. After you delete the temporary files, go back and check the remaining contents of the folder in Windows Explorer. Note that only cookie files remain. They sometimes give clues about the sites that you have visited, and you should also review those to decide which cookies to keep and which ones to delete.

An alternative method for opening the Internet Options dialog box is as follows: Go to Control Panel and double click on the Internet Properties icon. In the Internet Properties dialog box under the General Tab, click on Delete Files in the Temporary Internet Files section. To open Control Panel click Start on your Desktop and point to Settings, then click Control Panel.

Outlook Express Mail and Newsgroups

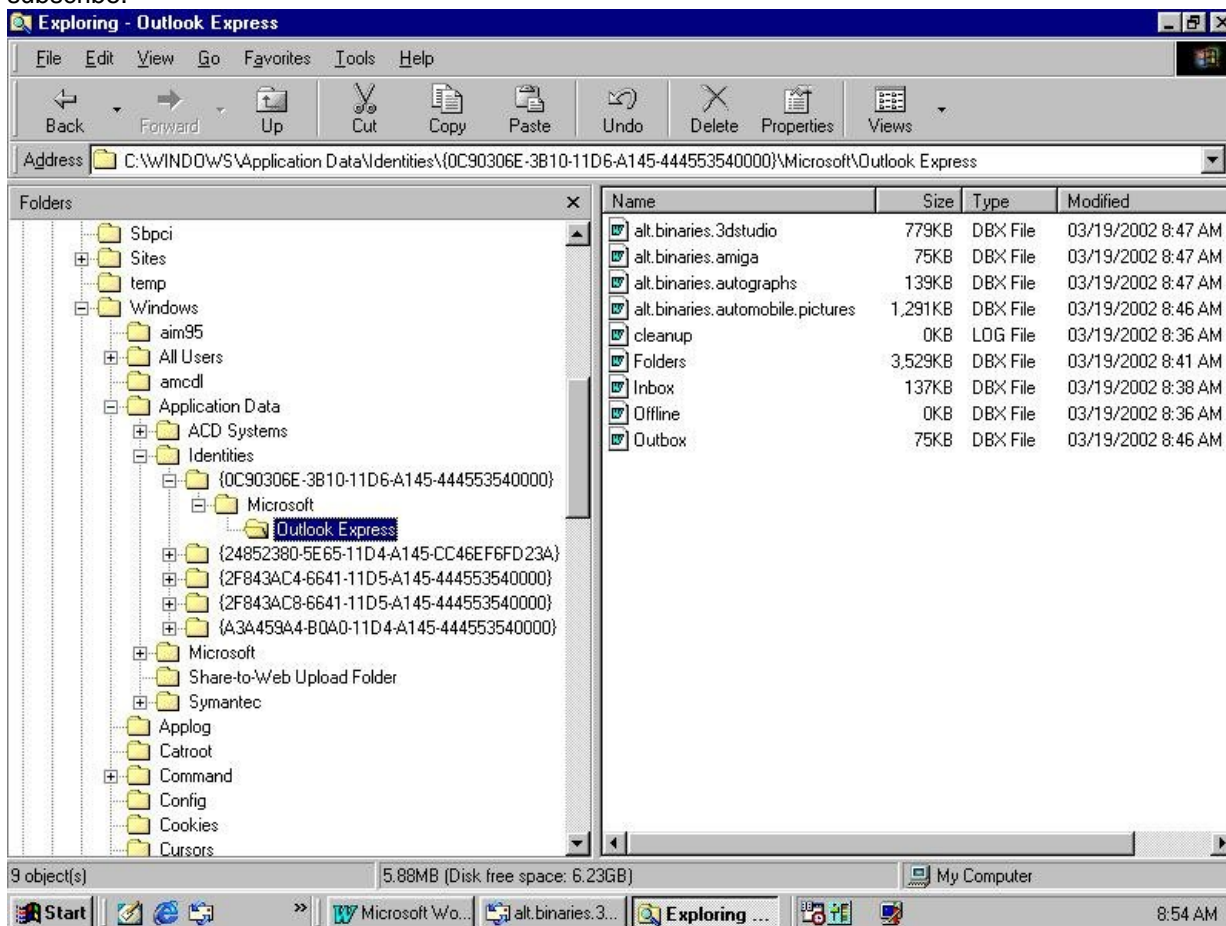
Many Internet Explorer users also use Outlook Express as their main email program. If you do, and you send and receive sensitive or compromising messages, please be aware that Windows creates a history of all your email folders and messages. Those files are located at: C:\WINDOWS\Application Data\Identities. 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.



Recycle Bin

When you deleted files using the steps explained above, the files were removed from the Windows Explorer folders and sent to the Recycle Bin. **Check the Recycle Bin and delete selected, sensitive files after each session.** Here's one way to delete the files from the Recycle Bin. Double click the Recycle Bin icon on your Desktop to open that window. Click on Empty Recycle Bin to delete all items and reclaim disk space. Be aware that even though the files are deleted, they still reside on your hard drive and can be recovered and read. Cleaning your hard drive, which is the last step needed to complete the entire privacy program, is discussed in the PC Privacy Protection Program Guide.

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 need, or programs that you no longer use. Under the Settings tab, you can also select an option to run Disk Cleanup if the drive runs low on disk space at any time.

Hard Drive/ Disk Cleanup

Introduction

There is good news – it's not as hard as it seems to clean your PC. 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. The programs are **East-Tec Eraser, DisposeSecure, and other hard drive wipers that are available on the Internet.**

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.

Cleaning Up Your PC and Hard Drive

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. **Run Computer and hard drive wiper software after each session.** They will destroy 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. These 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. Most decent eraser programs are fully integrated with the Window's shell, so you can erase files directly from Explorer or My Computer, with a single mouse click. They are also designed to support almost any operating system available today.

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 on all disks and removable media.** Normal formatting DOES NOT erase disk data beyond recovery. There are a number of 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 such software 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 an eraser product on your hard drive prior to resale, lease return, donation or disposal of your old PC.** They offer an easy and quick 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.

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 lock / access control software.** They provide 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 image 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 a number of programs that can do the job for you. A quick search on the Internet will give you many options to choose from. Once installed, these programs will protect sensitive information from use or abuse by others with access to your PC. They will also hide your personal and confidential folders and make them visible and available to you ONLY! Some will change their attributes to prevent unauthorized use or abuse, such as reading, deleting, renaming, modifying, executing or corrupting and/or 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 and use anonymous surfing software for Internet security protection.** Anonymous surfing allows you to enjoy the Internet and send Email anonymously. It makes you invisible to online snoops and shields you from malicious code, web bugs, viruses, cookies, and more. Certain programs also encrypt and protect 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. These programs can create an impenetrable virtual tunnel between your computer and the Internet world using protected servers with SSH encryption. This protects you across untrusted networks and ISPs, and defends against even the most sophisticated snooping methods. Some other basic services are:

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

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.) snoops 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 snoops 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 anti-spy 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. Such programs are essential 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](#). These helpful programs will stop annoying popups and saves bandwidth. Get the latest in intelligent popup software that kills ad popups. They all 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](#).

Many anti-spam agents are available to deal with the latest in email spam technology. 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 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 credit card information on your PC. Using Internet Explorer AutoComplete fields makes you particularly vulnerable. [Purchase software to protect you from credit card fraud](#).

Programs that secure your private information offer highly effective security for Internet Explorer 5.0 and above. They provide credit card online security by scanning Internet Explorer autocomplete fields for credit card numbers and removing them. Eliminate any worry about Internet Explorer security or using the convenient autocomplete feature. Secure your credit card numbers and protect them from exposure to theft on the Internet.

Internet Explorer Cleanup – Summary of Clean Up Steps and Required Software:

Clear the Address Window after each session.
Check the Favorites list frequently and delete items that should not appear there.
Clear Internet Explorer History after each session.
Clear (delete) all files in the Windows/History/Today folders after each session.
Clear the IE History to eliminate the visited link colors trail.
Check and clean out Temporary Internet Files often.
Clean out the contents of Outlook Express email folders on a regular basis.
Periodically review and clean out the Identity folder containing newsgroup files.
Check the Recycle Bin and delete selected, sensitive files after each session.
Use Disk Cleanup for [C:] to clean certain Windows files simultaneously.
Run a hard drive eraser program after each session.
Run a wiping software on all disks and removable media.
Run a hard drive sanitizer program prior to resale, lease return, donation or disposal of your old PC.

Software Required to Protect PC Privacy and Internet Security

PC Access Control – Password protect your PC.
Purchase and use a computer locking software / PC access control software for access control.
File and Folder Protection - Purchase and use privacy software to protect your files and folders.
Anonymous Internet Connections - Purchase anonymous surfing software for Internet security protection.
Hacker Protection - Purchase firewall protection to stop snoops and hackers.
Anti spy software protection - Run anti-spy programs periodically.
Purchase an effective popup and ad blocking software.
Purchase an anti-spam program to fight Spam with the click of a button.
Purchase a privacy program to secure credit card and other personal information.

- The End -