

How to Secure Windows and Your Privacy

-- with Free Software

An Easy Guide for the Windows User

By Howard Fosdick
Fosdick Consulting Inc.

© 2008 July 26

Version 2.1

Distribution: You may freely reproduce and distribute this guide however you like – but you may not change its contents in any way.

This product is distributed at no cost under the terms of the [Open Publication License](#) with License Option A --
“Distribution of modified versions of this document is prohibited without the explicit permission of the copyright holder.”

Feedback: Please send recommendations for improving this guide to the author at email address “ContactFCI” at the domain name “sbcglobal.net”. **Disclaimer:** This paper is provided without warranty. Fosdick Consulting Inc. and the author accept no responsibility for any use of the data contained herein. **Trademarks:** All trademarks included in this document are the property of their respective owners.

About the Author: Howard Fosdick is an independent consultant who works hands-on with databases and operating systems. He’s written many articles, presented at conferences, founded software users groups, and invented concepts like *hype curves* and *open consulting*.

Acknowledgments: Thank you to the reviewers without whose expert feedback this guide could not have been developed: Bill Backs, Huw Collingbourne, Rich Kurtz, Priscilla Polk, Janet Rizner, and others who prefer anonymity. Thank you also to the Association of PC Users (APCU), Better Software Association, BitWise Magazine, IBM Database Magazine, OS News, Privacy Rights Clearinghouse, TechRepublic, UniForum, and ZDNet. Finally, thank you to the hundreds of readers who provided feedback.

Do you know that --

- ❑ Windows secretly records all the web sites you've ever visited?
- ❑ After you delete your Outlook emails and empty the Waste Basket, someone could still read your email?
- ❑ After you delete a file and empty the Recycle Bin, the file still exists?
- ❑ Your Internet Service Provider may compile a complete dossier on your web surfing?
- ❑ Your computer might be a *bot*, a slave computer waiting to perform tasks assigned by a remote master?
- ❑ Microsoft Word and Excel documents contain secret keys that uniquely identify you?
- ❑ Office also collects statistics anyone can read on how long you spent working on documents and when?

This guide explains these – and many other -- threats to your security and privacy when you use Windows computers. It describes these concerns in simple, non-technical terms. The goal is to provide information anyone can understand.

This guide also offers solutions: safe practices you can follow, and free programs you can install. Download links appear for the free programs as they are cited.

No one can guarantee the security and privacy of your Windows computer. Achieving foolproof security and privacy with Windows is difficult. Even most computer professionals don't have this expertise.

Instead, this guide addresses the security and privacy needs of most Windows users, most of the time. Follow its recommendations and your chances of a security or privacy problem will be minimal.

Since this guide leaves out technical details and obscure threats, it includes a detailed Appendix. Look there first for deeper explanations and links to more information.

Why Security and Privacy Matter

Why should you care about making Windows secure and private? Once young “hackers” tried to breach Windows security for thrills. But today penetrating Windows computers yields big money. So professional criminals have moved in, including overseas gangs and organized crime.

All intend to make money off you – or anyone else who does not know how to secure Windows. Security threats are increasing exponentially.

This guide tells you how to defend yourself against those trying to steal your passwords, personal data, and financial information. It helps you secure your Windows system from outside manipulation or even destruction.

It also helps you deal with [corporations](#) and [governments](#) that breach Windows security and your privacy for their own ends. You have [privacy](#) if only **you** determine when, how, and to whom your personal information is communicated. Organizations try to gain advantage by eliminating your privacy. This guide helps you defend it.

The Threats

Windows security and privacy concerns fall into three categories --

1. How to defend your computer against outside penetration attempts
2. How Windows tracks your behavior – and how to stop it
3. How to protect your privacy when using the Internet

The first two threats are specific to Windows computers. The last one applies to the use of any kind of computer. These three points comprise the outline to this guide.

Outline

1. How to Defend Against Penetration Attempts	4
1.1 Act Safely Online	4
1.2 Install Self-Defense Software	4
Firewall	
Anti-Virus	
Anti-Malware	
Anti-Rootkit	
Intrusion Prevention	
1.3 Keep Your Programs Up-to-Date!	7
1.4 Test Your Computer's Defenses	8
1.5 Peer-to-Peer Programs Can Be Risky.	9
1.6 Don't Let Another User Compromise Your Computer	10
1.7 Use <i>Administrator</i> Rights Sparingly	10
1.8 Use Strong Passwords	11
1.9 Always Back Up Your Data	11
1.10 Encrypt Your Data	12
1.11 Reduce Browser Vulnerabilities	12
Will Your Browser Run <i>Anybody's</i> Program?	
Internet Explorer Vulnerabilities	
1.12 Wireless Risks	13
1.13 Replace Microsoft Products?	14
2. How Windows Tracks Your Behavior – and How to Stop It	15
2.1 How to Securely Delete Data	15
How to Securely Delete Files	
How to Securely Delete Email and Address Books	
How to Securely Delete All Personal Data on Your Computer	
2.2 The Registry Contains Personal Data	17
2.3 Windows Tracks All the Web Sites You've Ever Visited	18
2.4 Windows Leaves Your Personal Information in its Temporary Files	19
2.5 Your "Most-Recently Used" Lists Show What You're Working On	20
2.6 Product Registration Information May be Hard to Change	20
2.7 File "Properties" Expose Personal Data	20
2.8 Microsoft Embeds Secret Identifiers in Your Documents	22
2.9 Windows Secretly Contacts Microsoft	23
2.10 Chart of Microsoft's Tracking Technologies	23
2.11 Does Your Printer Spy on You?	24
3. How to Protect Your Privacy When Using the Internet	25
3.1 Limit the Personal Information You Give Out	25
3.2 Don't Let Web Sites Track You	26
3.3 Is Your Email Private?	27
3.4 Is Your Web Surfing Private?	29
3.5 Are Your Web Searches Private?	30
4. Wisdom	32
5. Appendix – Further Information and Links	33

1. How to Defend Against Penetration Attempts

There are many reasons someone or some organization out in the Internet might want to penetrate your Windows computer. Here are a few examples –

- ❑ To secretly install software that steals your passwords or financial information
- ❑ To enroll your computer as a *bot* that secretly sends out junk email or *spam*
- ❑ To implant software that tracks your personal web surfing habits
- ❑ To destroy programs or data on your PC

Your goals are to—

- ❑ Prevent installation of malicious software or [malware](#)
- ❑ Identify and eliminate any malware that does get installed
- ❑ Prevent malware from sending information from your computer out into the web
- ❑ Prevent any other secret penetration of your computer

1.1 Act Safely Online

Let's start with the basics. *Your use of your computer -- your online behavior – significantly affects how easy it is to penetrate your PC.*

Practice safe web surfing. Handle your email safely. Follow these tips to reduce the chances that outsiders can penetrate your computer:

- ❑ Don't download free screensavers, wallpaper, games, or toolbars unless you know they're safe. These often come with embedded malware. If you just can't pass up freebies, download them to a directory where you scan them with your anti-virus and anti-malware programs before using them.
- ❑ Don't visit questionable web sites. Hacker sites, sexually explicit sites, and sites that engage in illegal activity like piracy of music, videos, or software are well known for malware. You could get hit by a [drive-by](#) -- a malicious program that runs just by virtue of your viewing a web page.
- ❑ Don't open email or email attachments from questionable sources. These might install malware on your system. Dangerous email attachments often present themselves as games, interesting pictures, electronic greeting cards, or invoices so that you will open them. (If you get too much junk email, reduce it with [these free programs](#).)
- ❑ Don't click on links provided in emails. These could direct you to a legitimate-looking but bogus web site designed to steal your personal information. *Companies that protect their customers don't conduct business through embedded links in emails!*
- ❑ Before you enter your online account name and password into any web site, be sure the web page is secure. The web page's address should start with the letters **https** (rather than **http**). Most browsers display a closed lock icon at the bottom of the browser panel to indicate a secure web site form.
- ❑ Don't give out your full name, address, phone number, or other personal information in chat rooms, forums, on web forms, or in social networks. (Section 3 on "How to Protect Your Privacy When Using the Internet" has more on this topic.)
- ❑ The Appendix links to articles with more safety tips.

1.2 Install Self-Defense Software

To defend Windows, you need to install software that protects against several kinds of threats. This section describes the threats and the software that defends against each.

Some programs provide protection against multiple threats. *But no single program protects you from all threats!*

Compare any protective software you already have installed to what I describe below. To cover any gaps, I recommend free software you can download and install. The discussion includes download links for the free programs.

Figure 1 – Download any of the free programs in this guide from [TheFreeCountry.org](http://www.thefreecountry.org), [Download.com](http://www.download.com), or [Major Geeks](http://www.majorgeeks.com). Here is the main panel for free security programs at [TheFreeCountry.org](http://www.thefreecountry.org) ...



Firewall – [Firewalls](#) are programs that prevent data from coming into or leaving from your computer without your permission. Unsolicited data coming into your computer could be an attempt to compromise it; unauthorized data leaving your computer may be an attempt to secretly steal your data or spy on your activities.

Every Windows computer should run a firewall at all times when it is connected to the Internet.

Windows ME, 98, and 95 did not come with a firewall. XP and Vista do. However, the XP and Vista firewalls have shortcomings.

The [XP firewalls](#) (there are actually two versions) do not stop unauthorized outgoing data. This is unacceptable because if malware somehow got installed on your computer, it could send data out

without you realizing it.

[Vista's built-in firewall](#) can stop unauthorized outbound data but it does not do so by default. [This how-to article](#) shows that enabling this critical feature is not easy.

If you run XP or older Windows versions, install a free firewall and use it instead of Microsoft's. If you run Vista, either download a free firewall or take the time to [properly configure Vista's](#).

Good free firewalls include [ZoneAlarm](#), [Comodo Firewall](#), [Sygate Personal Firewall](#), or [Jetico Personal Firewall](#). ZoneAlarm is especially easy to set up, since it is self-configuring. Find other free firewalls along with a quick comparative review [here](#). See the Appendix for more details about firewalls.

Anti-Virus – [Viruses](#) are programs that are installed on your computer without your knowledge or permission. The damage they do ranges from acting as a nuisance and wasting your computer's resources, all the way up to destroying your data or Windows itself.

Anti-virus programs help identify and eliminate viruses that get into your computer. Free anti-virus programs include [AVG Anti-Virus](#), [avast! Anti-Virus Home Edition](#), and [PC Tools Anti-Virus Free Edition](#). If you don't already have an anti-virus scanner, download and install one of these, then run it regularly to scan your disk for any viruses. You can schedule the program to run automatically either through its own built-in scheduling facility or through the [Windows Scheduler](#).

Good anti-virus programs like these automatically scan data as it downloads into your computer. This includes emails you receive and any files you download.

Anti-Malware -- In addition to viruses, there are many other kinds of programs that try to secretly install themselves on your computer. Generically, they're called [malware](#). They include:

<i>Spyware</i>	It spies on your behavior and sends this data to a remote computer
<i>Adware</i>	It targets you for advertisements
<i>Trojans</i>	These scam their way into your computer
<i>Rootkits</i>	These take over <i>administrator rights</i> and can do anything to your PC
<i>Dialers</i>	These secretly use your communication facilities
<i>Keyloggers</i>	These record your keystrokes (including passwords) and send this data to a remote computer
<i>Botware</i>	Your computer becomes a <i>bot</i> or <i>zombie</i> , ready to carry out secret orders

Since no one program identifies and removes all kinds of malware, you need a couple in addition to your anti-virus scanner. Free programs for this purpose include [Ad-Aware Free](#), [Spybot Search and Destroy](#), and [a-Squared Free Anti-Malware](#). I recommend running two anti-malware programs on a regularly-scheduled basis.

Anti-Rootkit -- [Rootkits](#) are a particularly vicious form of malware. They take over the master or *Administrator* user rights on your PC and therefore are very effective at hiding themselves.

Many of the anti-malware programs above provide some protection against rootkits. But sometimes a specialized detection program is useful. Rootkit detectors often require technical expertise but I can recommend [Sophos Anti-Rootkit](#) as easy-to-use. It requires Windows XP or 2000 or newer.

Intrusion Prevention – [Intrusion detection programs](#) alert you if some outside program tries to secretly enter Windows by replacing a program on your computer. For example, an outside program might try to replace part of Windows or alter a program such as Internet Explorer.

Free intrusion detection programs include [WinPatrol](#), [SpywareGuard](#), [ThreatFire Free Edition](#), and [ProcessGuard Free](#). Install one of them and it will run constantly in the background on your computer, detecting and preventing intrusions.

1.3 Keep Your Programs Up-to-Date!

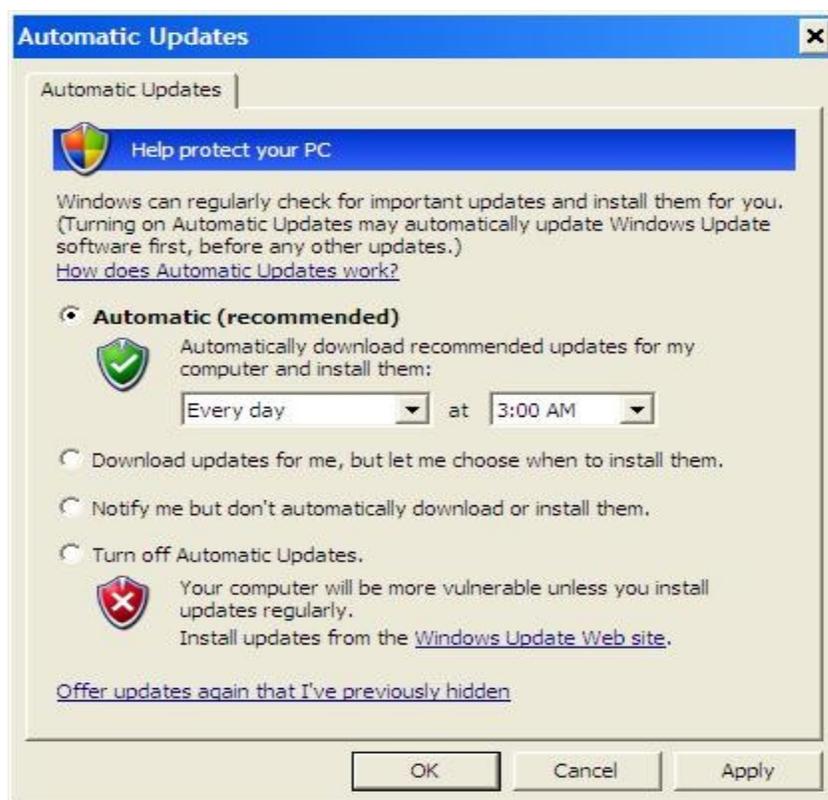
All anti-malware programs require frequent updating. This enables them to recognize new kinds of malware as they are developed. The programs listed above automatically check for updates and download and install them as needed. (Each has a panel where you can verify this feature.)

You must also keep Windows up-to-date. In Vista, the automatic feature for this purpose is called [Windows Update](#). It is on by default. You can manage it through the *Control Panel | Security | Windows Update* option.

As Microsoft [explains](#), they have broadened *Windows Update* into a facility they call *Microsoft Update*. The latter auto-updates a broader range of Microsoft products than does Windows Update. For example, it updates Microsoft Office. You can sign up for Microsoft Update at the [Microsoft Update web site](#).

In XP and Windows 2000, the auto-update feature was usually referred to as [Automatic Updates](#). Manage it through *Control Panel | Automatic Updates*.

Figure 2 – Ensuring Automatic Updates are enabled in Windows XP ...

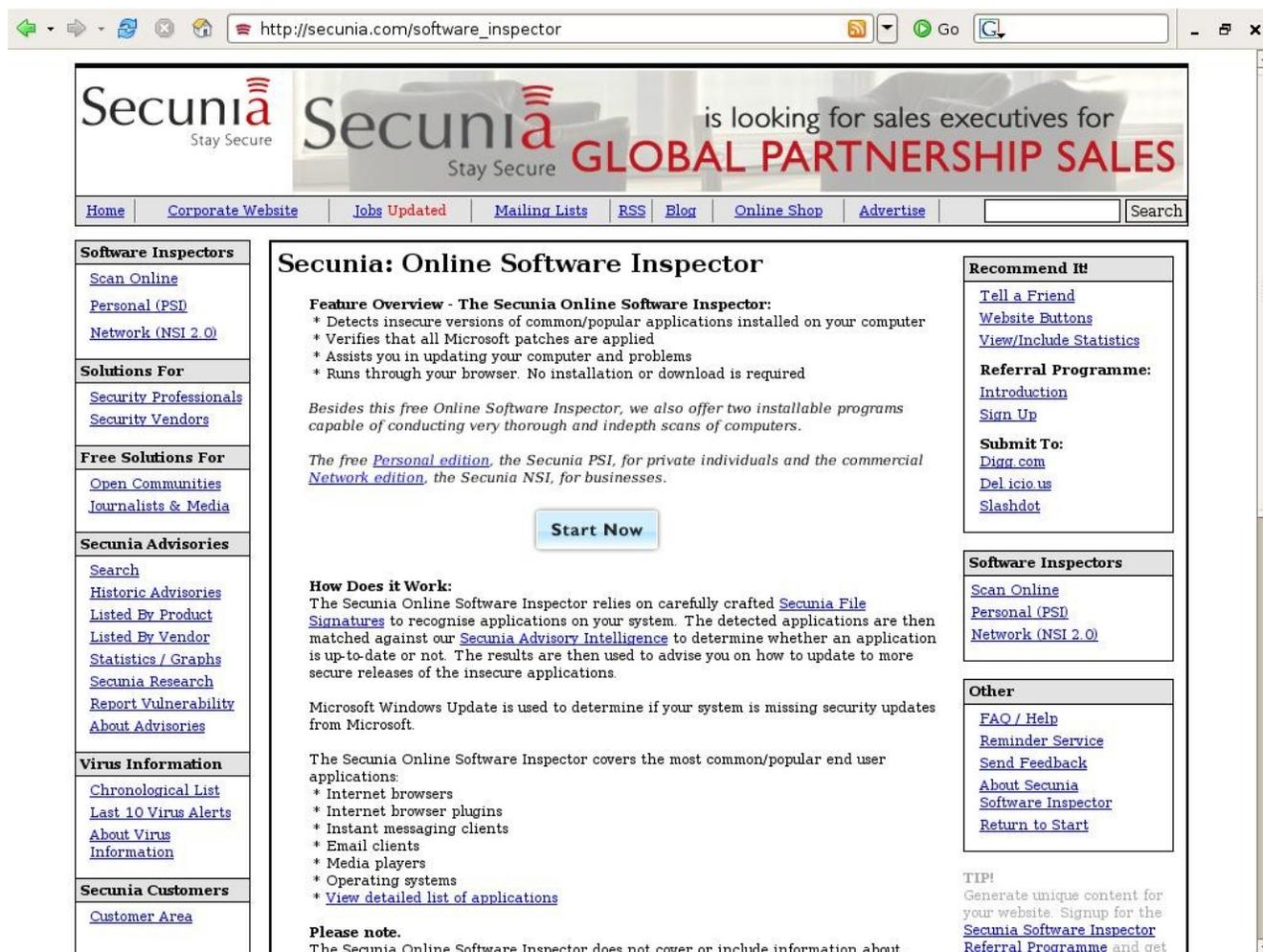


Beyond Windows, you must also keep the major applications on your computer up-to-date. Examples are Adobe's Flash Player, Firefox, and RealPlayer. Most default to automatic updating. *It's a good practice to verify the auto-update setting right after you install any new program.* Then you never need check it again.

If you don't know whether your system has all the required updates for your programs, run the free [Secunia Software Inspector](#). It detects and reports on out-of-date programs and ensures all "bug fixes" are applied.

If you need to download software updates for many programs, [The Software Patch](#) allows you to download them all through one web site.

Figure 3 – Scan for all programs requiring update at [Secunia.com](#) ...



1.4 Test Your Computer's Defenses

You can test how well your computer resists penetration attempts by running the free [ShieldsUp! program](#). ShieldsUp! tells you about any security flaws it finds. It also displays the system information your computer gives out to every web site you visit. Section 3 on "How to Protect Your Privacy When Using the Internet" addresses this privacy concern.

Test whether your computer's firewall stops unauthorized outgoing data by running the free program [LeakTest](#).

Figure 4 – Test your computer's defenses with [ShieldsUp!](#) ...



1.5 Peer-to-Peer Programs Can Be Risky

[Peer-to-peer programs](#) share music, videos and software. Popular examples include BitTorrent, Morpheus, Kazaa, Napster, and Gnutella. Peer-to-peer (or P2P) networking makes it possible for you to easily download files from any of the thousands of other personal computers in the network.

The problem is that by using peer-to-peer programs, you agree to allow others to read files from **your** computer. *Be sure that only a single Folder on your computer is shared to the Internet, not your entire disk!* Then, be very careful about what you place into that shared Folder.

Some peer-to-peer programs use the lure of the free to implant adware or spyware on your computer. Other P2P systems engage in theft because they “share” files illegally.

The popular [PC Pitstop web site](#) tested major P2P programs for bundled malware in July 2005 and here's what they found –

P2P Program:	Adware or Spyware Installed:
Kazaa	Brilliant Digital, Gator, Joltid, TopSearch
Ares	NavExcel Toolbar
Bearshare	WhenU SaveNow, WhenU Weather
Morpheus	PIB Toolbar, Huntbar Toolbar, NEO Toolbar
Imesh	Ezula, Gator
Shareaza, WinMX, Emule, LimeWire, BitTorrent, BitTornado	None

The [PC Tools Software web site](#) tracks P2P infections [here](#).

*If you decide to install any peer-to-peer program, determine if the P2P program comes with malware **before** you install it.*

You greatly increase your personal security by not getting involved in the illegal sharing of music, videos, and software. *File "sharing" in violation of copyright is theft.* The [Recording Industry Association of America](#) has sued over 20,000 people for it as of mid-2006.

1.6 Don't Let Another User Compromise Your Computer

Got kids in the house? A teen or younger child might violate the "safe surfing" rules above and you wouldn't know it.... until you get blindsided by malware the next time you use your computer.

[This article](#) tells about a couple whose tax returns and banking data ended up on the web after their kids used P2P networking software the parents didn't even know was installed. A spouse or friend could cause you the same grief.

If you are not the sole user of your computer -- or if you do not feel completely confident that your computer is secure -- consider what personal information you store. Do you really want to manage your credit cards, bank accounts or mutual funds from your PC? *Only if you know it's secure!* (Read the agreements for online financial services and you'll see that **you** are responsible for security breaches that compromise your accounts.)

Some families use two computers: one for the kids and a secure one for the adults. They use the less secure computer for games and web surfing, and carefully restrict the use of the more secure machine. This two-computer strategy is appealing because today you can buy a used computer for only a hundred dollars.

An alternative is to share one computer among everyone but set up separate user ids with different [access rights](#) (explained below). Ensure that only a single user id has the authority to make changes to Windows and restrict its use.

Never use a public computer at a computer cafe or the library for online finances or other activities you must keep secure.

1.7 Use Administrator Rights Sparingly

To install programs or perform security-sensitive activities on a Windows computer requires [administrator rights](#). When you use administrator rights, any malware program you accidentally or unknowingly run has these rights -- and can do anything on your system.

In systems like Windows XP and Windows 2000, the built-in *Administrator* user id inherently has administrator rights. You can also create other user ids to which you assign administrator rights.

Working full-time with a user id that has administrator rights makes you vulnerable! In contrast, using an account that does not have administrator rights gives you a great deal of protection. So create a new user id without administrator rights and use it. Then use the *Administrator* id only when necessary.

Windows Vista introduces a new feature called [user account control](#) that helps you avoid using administrator rights except when required. This feature prompts you to enter a password when you want to perform any action that requires administrator rights. While entering passwords may seem like a hassle, UAC is a big step towards a more secure Windows. Here is Microsoft's [introductory guide](#) on this feature.

Early Windows versions – ME, 98, and 95 – don't have a system of access rights. Whatever user id you use has the administrator powers. To keep these systems secure, all you can do is follow the other recommendations in this guide very carefully.

1.8 Use Strong Passwords

Passwords are the front door into your computer – and any online accounts you have on the web. You need to:

- Create strong passwords
- Change them regularly
- Use different passwords for different accounts

Strong passwords are random mixes of letters, numbers, and punctuation (if allowed) that contain eight or more characters:

AlbqP_1793, pp30-Mow9, PPw9a3mc84

Weak passwords are composed of personal names or words you can find in the dictionary:

Polly28, Bigdog, alphahouse, wisewoman2, PhoebeJane

If keeping track of different passwords for many different accounts strikes you as impractical (or drives you nuts!) you might try a "password management" tool from any of the dozen free products listed [here](#).

If you set up a home wireless network, be sure to assign the router a password!

1.9 Always Back Up Your Data

One day you turn on your computer and it won't start. Yikes! What now?

If you backed up your data, you won't lose it no matter what the problem is. *Backing up data is simple*. For example, keep all your Word documents in a single Folder, then write that Folder to a plug-in USB memory stick after you update the documents. Or, write out all your data Folders once a week to a writeable CD.

For the few minutes it takes to make a backup, you'll insure your data against a system meltdown. This also protects you if malware corrupts or destroys what's on your disk drive.

If you didn't back up your data and you have a system problem, you can still recover your data as long as the disk drive still works and the data files are not corrupted. You could, for example, take the disk drive out of the computer and place it into another Windows machine as its second drive. Then read your data -- *and back it up!*

If the problem is that Windows won't start up, the web offers tons of advice on how to fix and start Windows (see the Appendix). Another option is to start the machine using a Linux operating system CD and use Linux to read and save data from your Windows disk.

If the problem is that the disk drive itself fails, you'll need your data backup. If you didn't make one, your only option is to remove the drive and send it to a service that uses forensics to recover data. This is expensive and may or may not be able to restore your data. *Learn the lesson from this guide rather than from experience – back up your data!*

1.10 Encrypt Your Data

Even if you have locked your Windows system with a good password, anyone with physical access to your computer can still read the data!

One easy way to do this is simply to boot up the Linux operating system using a CD, then read the Windows files with Linux. This circumvents the Windows password that otherwise protects the files.

Modern versions of Windows like [Vista](#) and [XP](#) include *built-in encryption*. Right-click on either a Folder or File to see its *Properties*. The Properties' *Advanced* button allows you to specify that all the files in the Folder or the single File will be automatically encrypted and decrypted for you. This protects that data from being read even if someone circumvents your Windows password. It is sufficient protection for most situations.

Alternatively, you might install free encryption software like [TrueCrypt](#), [BestCrypt](#) or [many others](#).

If you encrypt your data, be sure you will always be able to decrypt it! If the encryption is based on a key you enter, you must remember the key. If the encryption is based on an *encryption certificate*, be sure to back up or "export" the certificates, as described [here](#). You might wish to keep unencrypted backups of your data on CD or USB memory stick.

Laptop and notebook computers are most at risk to physical access by an outsider because they are most frequently lost or stolen -- keep all data files your portable computer encrypted.

1.11 Reduce Browser Vulnerabilities

As the program you run to access the Internet, your [web browser](#) is either your first line of defense or a key vulnerability in protecting your computer from Internet malware.

Will Your Browser Run *Anybody's* Program? - From a security standpoint, the worldwide web has a basic design flaw – *many web sites expect to be able to run any program they want on your personal computer*. **You** are expected to accept the risk of running their code! The risk stems from both accidental program defects and purposefully malicious code.

Some web sites require that you allow their programs to run their code to get full value from the web site. Others do not. You can find whether the web sites you visit require programmability simply by turning it off and visiting the site to see if it still works properly.

Here are the keywords to look for in web browsers to turn off their programmability --

- ActiveX*
- Active Scripting* (or *Scripting*)
- .NET components* (or *.NET Framework components*)
- Java* (or *Java VM*)
- JavaScript*

Turn off the programmability of your browser by un-checking those keywords at these menu options --

Browser:	How to Set Programmability:
Internet Explorer	Tools Internet Options Security Internet Custom Level
Firefox (version 2+)	Tools Options Content
Opera	Tools Preferences Advanced Content
K-Meleon	Edit Advanced Preferences JavaScript
SeaMonkey	Edit Preferences Advanced (Java) Scripts and Plugins (JavaScript)

Internet Explorer Vulnerabilities -- The Internet Explorer browser has historically been vulnerable to malware. Free programs like [SpywareBlaster](#), [SpywareGuard](#), [HijackThis](#), [BHODemon](#), and [others](#) help prevent and fix these problems.

Tracking Internet Explorer's vulnerabilities is time-consuming because criminals continually devise new "IE attacks." *If you use Internet Explorer, be sure you're using the latest version and that Windows' automatic update feature is enabled so that downloads will quickly fix any newly-discovered bug.*

Internet Explorer has traditionally been insecure measured against competing browsers. Some feel that IE versions 7 and 8 correct these problems, or that Vista's new way of interfacing with IE resolves them. Others disagree. If you wish to use some other browser the above chart lists free alternatives..

1.12 Wireless Risks

[Wireless communication](#) allows you to use the Internet from your computer without connecting it to a modem by a wire or cable. Sometimes called [Wi-Fi](#), wireless technology is very convenient because you can use your laptop from anywhere there is a invisible Internet connection or [hotspot](#). For example, you could use your laptop and the Internet from a cafe, hotel, restaurant, or library hotspot.

But wireless presents security concerns. *Most public hotspots are un-secured.* All your wireless transmissions at the hotspot are sent in unencrypted "clear text" (except for information on web pages whose addresses begin with **https**). Someone with a computer and the right software could scan and read what passes between your computer and the Internet.

Don't use public hotspots for Internet communications you need to keep secure (like your online banking).

Many people set up a wireless home network. You create your own local hotspot so that you can use your laptop anywhere in the house without a physical connection.

Home routers are insecure by default. *You must apply security to them.* Otherwise you might inadvertently create a public hotspot! Freeloaders on your home network could reduce the Internet performance you're paying for. Activities like illegal song downloads would likely be traced to **you**, not to the guilty party you've unknowingly allowed to use your network.

First, be sure the wireless equipment you use supports either the [802.11 G or 802.11 N standards](#). These secure wireless transmissions through [WPA \(Wi-Fi Protected Access\) or WPA2](#) encryption.

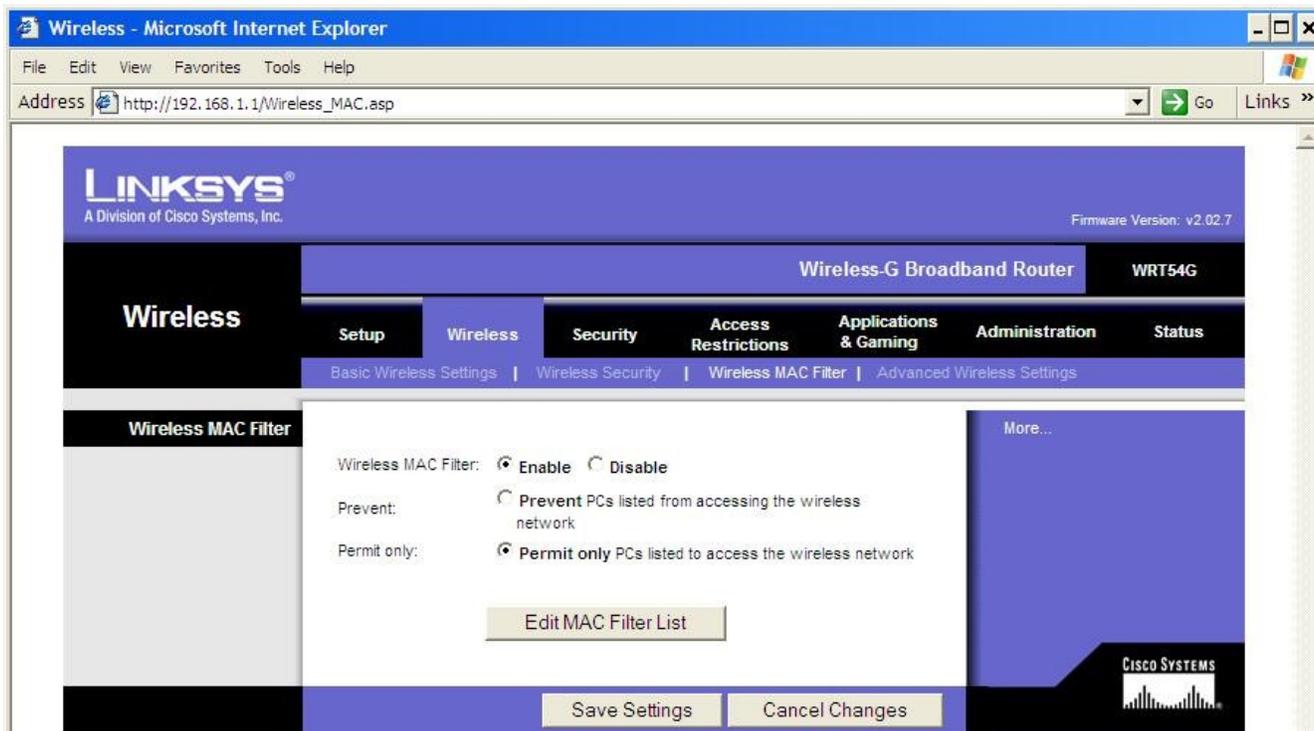
Do not base a wireless home network on equipment that only supports the older [802.11 A or 802.11 B standards](#). These use an encryption technology, called [WEP \(Wired Equivalent Privacy\)](#), that is **not** secure.

When you set up your wireless home network --

- Assign your system a unique name (don't use the default name)
- Tell the router not to broadcast that name
- Assign a tough new password to the router (don't use the default password!)
- Turn on the strongest encryption the router supports
- Restrict access to computers you specify through the feature called [MAC address filtering](#)
- Turn off the router and modem when you're not using them

Expert advice varies on how to best secure wireless networks, so see the Appendix for more detail.

Figure 5 – Access your router by typing its address into your browser. (Here I entered <http://192.168.1.1>). Most routers have tabbed panels that allow you to update key security parameters. Here I've restricted access to the modem to computers I specify by turning on the “Wireless MAC Filter” ...



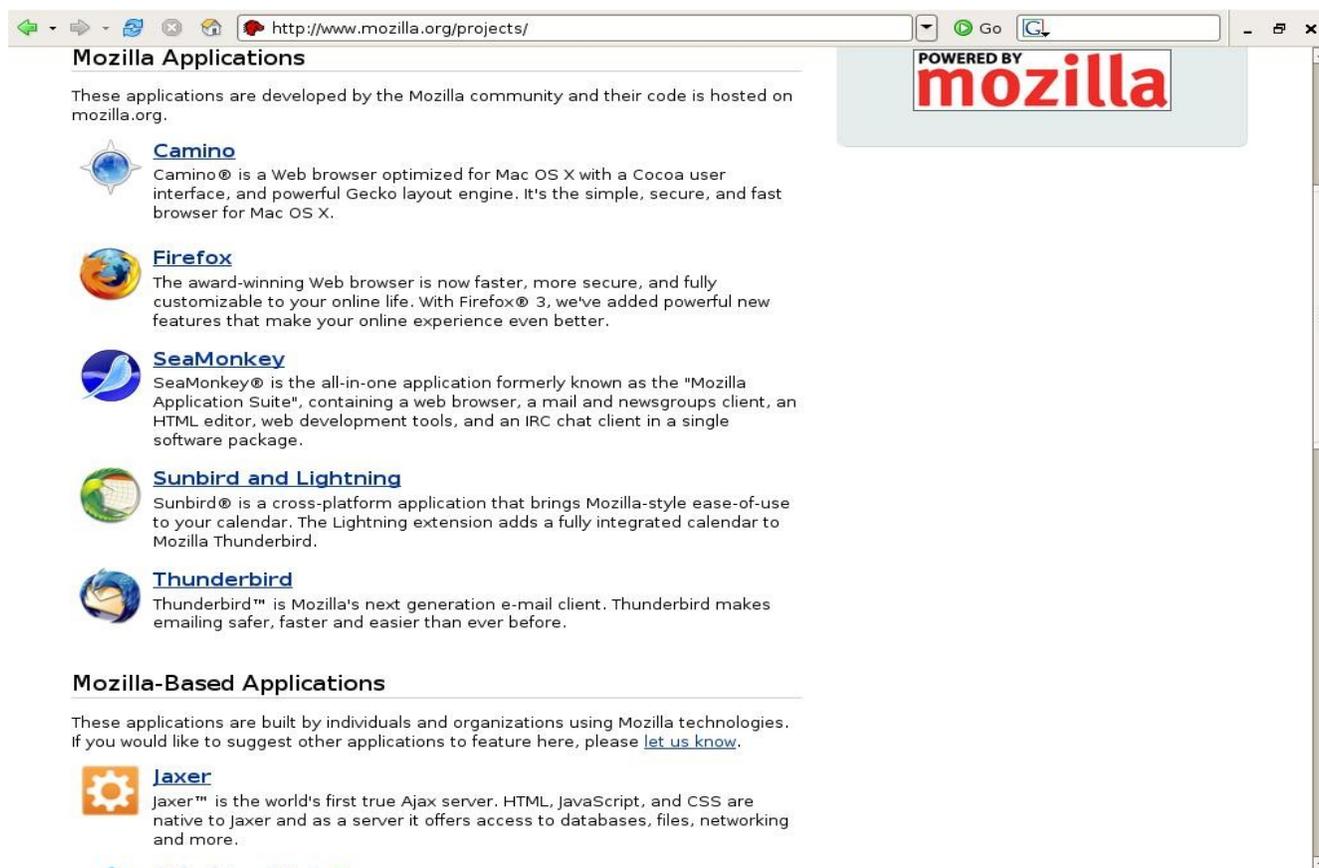
1.13 Replace Microsoft Products?

Talk to those who support computers for a living and you'll find that many consider two Microsoft products -- Internet Explorer and Outlook – malware magnets. One solution is to use free alternatives:

Product:	Alternatives:	See for Comparisons:	Explanation:
Internet Explorer	Firefox , Opera , others	Section 1.11, here and here	IE's poor security reputation is one reason 15% of Windows users now use Firefox
Outlook, Outlook Express	Thunderbird , Gmail , Yahoo mail	Here , here , here , and here	Avoid possible Outlook security issues by using other email clients or web mail
Office	OpenOffice	Section 2.7, 2.8, here , here , here and here	Security is fine with Office but privacy is lacking
Windows	Linux	Here , here , and here	Opinions differ greatly on how easy it is to switch systems and which is better

This guide focuses on Windows and Microsoft products so we don't much discuss alternatives. The topic falls outside the scope of this paper. Follow the links above if you want comparative product reviews.

Figure 6 – You can download free alternatives to Microsoft products at [Mozilla.org](http://www.mozilla.org) ...



2. How Windows Tracks Your Behavior – and How to Stop It

Are you aware that Windows tracks your behavior? It records all the web sites you ever visit, keeps track of all the documents you've worked on recently, embeds personal information into every document you create, and keeps Outlook email even if you tell Outlook to delete it. *These are just a few examples of many.*

This section first tells how to *securely delete* your files, folders, and email so that no one can ever retrieve them.

Then it describes the many ways in which Windows tracks your behavior. In some cases you can turn off this tracking. In most, your only option is to eliminate the tracking information after it has been collected.

2.1 How to Securely Delete Data

Let's start with how to permanently delete data from your computer.

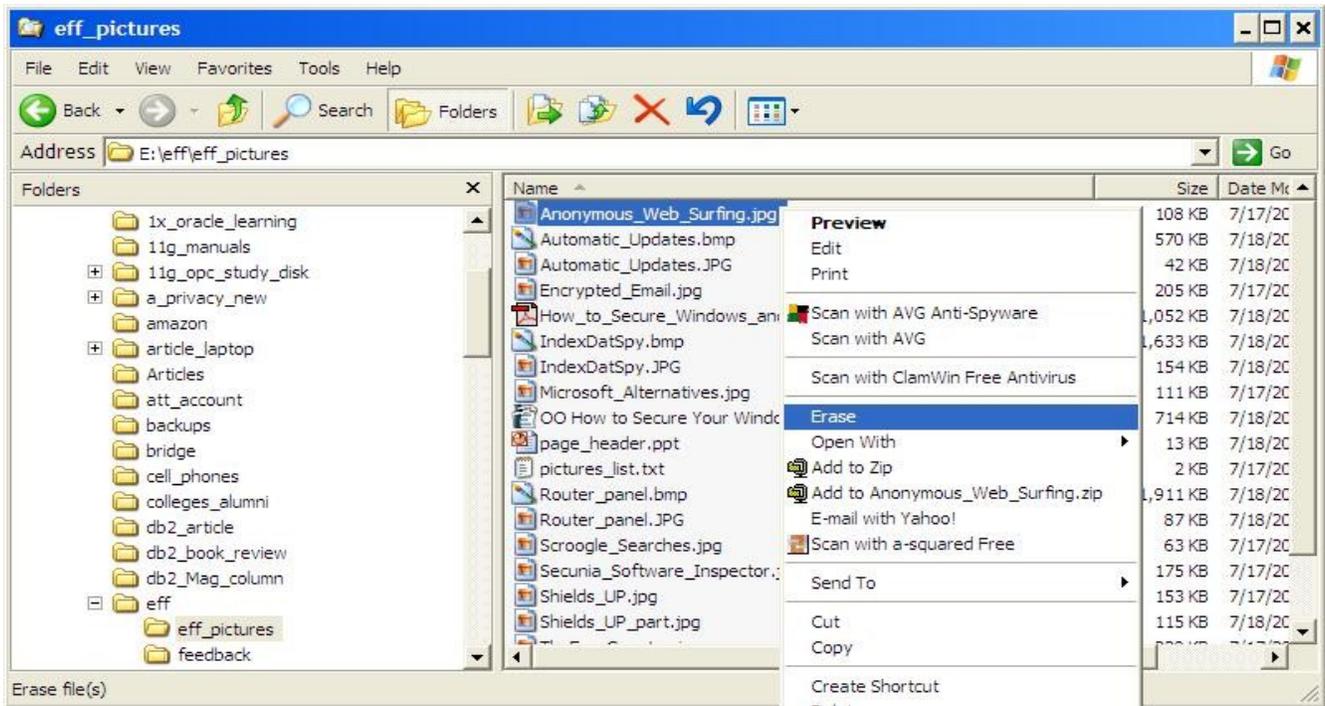
How to Securely Delete Files -- When you delete a file in Windows, Windows only removes the reference it uses to locate that file on disk. *Even after you empty the Recycle Bin, the file still resides on the disk.* It remains on the disk until some random time in the future when Windows re-uses this "unused" disk space.

This means that someone might be able to read some of your "deleted" files. (You can use free programs like [Undelete+](#) and [Free Undelete](#) to recover deleted files that are still on your disk.)

To *securely delete* files, you need to over-write them with zeroes or random data. Free programs that do this include [Eraser](#), [BCWipe](#), and [many others](#). After installing Eraser or BCWipe, you highlight a File or Folder, right-click the mouse, then select *Delete with Wiping* or *Erase* from the drop-down menu. This over-writes or *securely deletes* the data and so that it can never be read again.

Programs like [Eraser](#) and [BCWipe](#) also offer an option to over-write “all unused space” on a disk. This securely deletes any files you previously deleted using Windows Delete.

Figure 7 – Secure file deletion programs allow you to obliterate a file by right-clicking on the file name, then selecting the secure-deletion program from the resulting pop-up menu ...



How to Securely Delete Email and Address Books – Even after you delete your Outlook or Outlook Express emails and empty the email Waste Basket, files containing your emails remain to be read by someone later. What if you want to permanently delete all your emails so no one could ever read them?

Whether this is possible depends on whether your computer is stand-alone or part of an organizational network.

In an organizational setting, emails may be stored on central servers in addition to -- or instead of -- your personal computer. *Many organizations store all the emails you ever send or receive on their servers so that you can never delete them.* [Here](#) is a good discussion about whether you can really delete old emails in organizational settings.

If you have a stand-alone PC, emails are stored on your computer's hard disk. To securely erase emails residing on your computer, locate the Outlook or Outlook Express files that contain your emails. Then use a secure-erase tool like [Eraser](#) or [BCWipe](#) to permanently destroy them. You can do the same with your Windows address book.

The files you need to securely erase may be marked as *hidden files* within Windows. To work with

hidden files, you first need to make them visible. Checkmark *Show Hidden Files and Folders* under *Start | Settings | Control Panel | Folder Options | View*.

Now, search for file names having these *extensions* (ending characters) by using Windows' *Search* or *Find* facility --

.pst	Outlook emails, contacts, appointments, tasks, notes, and journal entries
.dbx or .mbx	Outlook Express emails
.wab	Windows address book file

Note that Outlook stores much other information in the same file along with your obsolete emails. You can either erase all that data along with your emails by securely deleting the file, or, [follow this procedure](#) to securely delete the email while retaining the other information.

For Outlook Express emails and Windows address books, just securely delete the files with the given extensions and you're done.

How to Securely Delete All Personal Data on Your Computer – How can you securely delete *all* your personal information on an old computer before giving it away or disposing of it? *This is difficult to achieve if you wish to preserve Windows and its installed programs.* It takes a lot of time and there is no single tool that performs this function.

The easiest solution is to overwrite the entire hard disk. This destroys all your personal information, wherever Windows hides it. Unfortunately it also destroys Windows itself and all its installed programs.

Be sure to copy whatever data you want to keep to another computer or storage medium first!

Several free programs securely overwrite your entire disk, such as [Darik's Boot and Nuke](#). The only possible way to recover data after running such programs is expensive physical analysis of the disk media, which may not be successful. Over-writing a disk is secure deletion for normal computer use.

2.2 The Registry Contains Personal Data

Windows keeps a central database of information crucial to its operations called the [Registry](#). Our interest in the Registry is that it stores your personal information. Examples include the information you enter when you register Windows and Office products like Word and Excel, lists of web sites you have visited, login profiles required for using various applications, and much more.

Upcoming sections discuss your personal information in the Registry how you can remove it. For now, let's just introduce a few useful Registry facts --

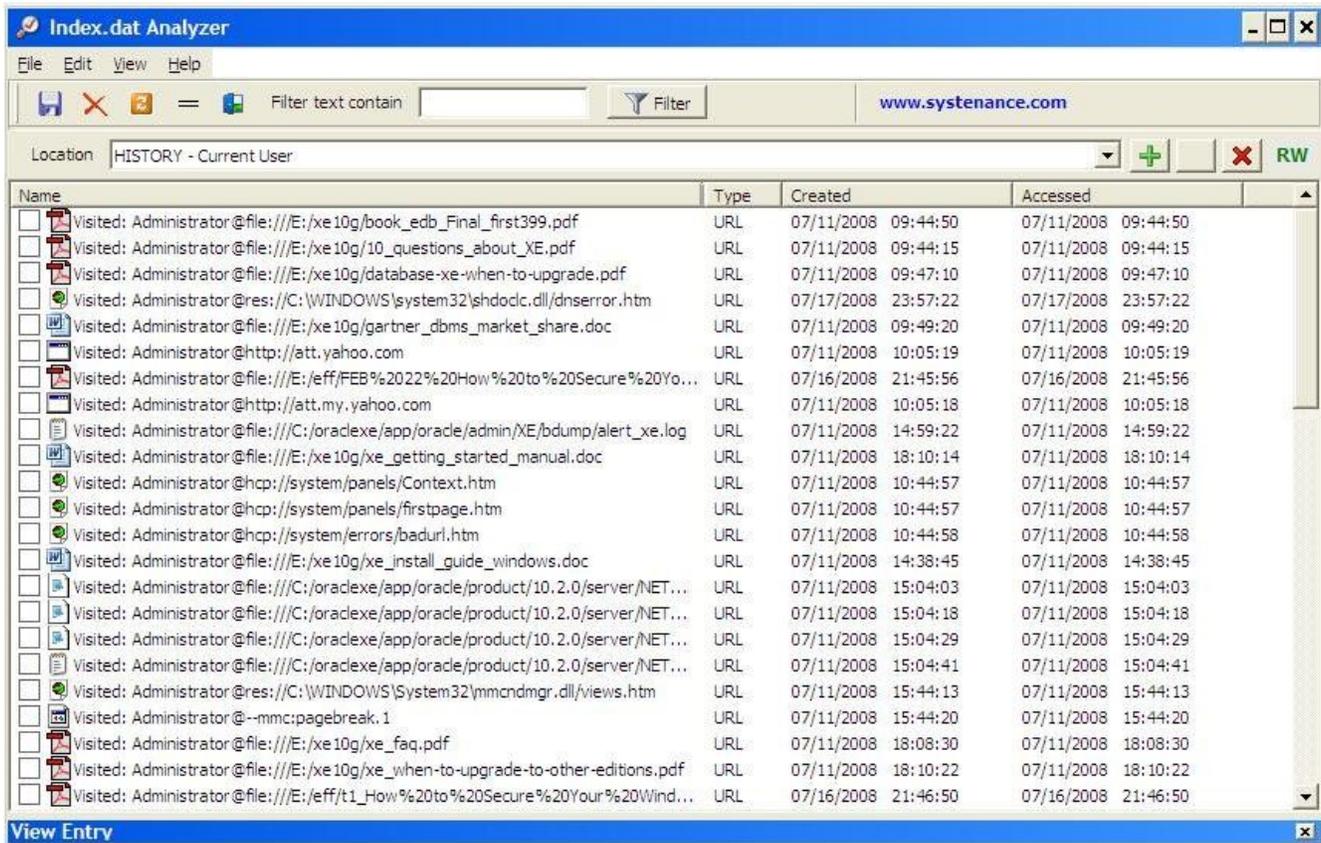
- The Registry is a large, complicated database (about which you can find tons of material on the web).
- The Registry consists of thousands of individual *entries*. Each *entry* consists of two parts, a *key* and a *value*. Each value is the setting for its associated key.
- The Registry organizes the entries into hierarchies.
- This guide tells how to change or remove your personal information in the Registry by running free programs, but it doesn't cover how to edit the Registry yourself – a technical topic beyond the scope of this paper.
- Making a mistake while editing the Registry could damage Windows, so you should only edit it if you feel well qualified to do so. Always make a backup before editing the Registry.*

2.3 Windows Tracks All the Web Sites You've Ever Visited

Windows keeps a list of all the web sites you've ever visited. You can tell Internet Explorer to eliminate this list through the IE selection *Tools | Internet Options | Clear History*. *But Windows still retains it!*

To view the web site history Windows retains, download and run a free program like [Index Dat Spy](#).

Figure 8 -- [Index Dat Spy](#) lists all the web sites you've ever visited...



Windows records your web surfing history in a file named **index.dat**. (There are actually several **index.dat** files on your computer ... I'll describe what the others track later.)

The **index.dat** files are special – you can not delete them or Windows will not start. Since Windows prevents you from changing or deleting these files, you need to run a free program to erase your web site history.

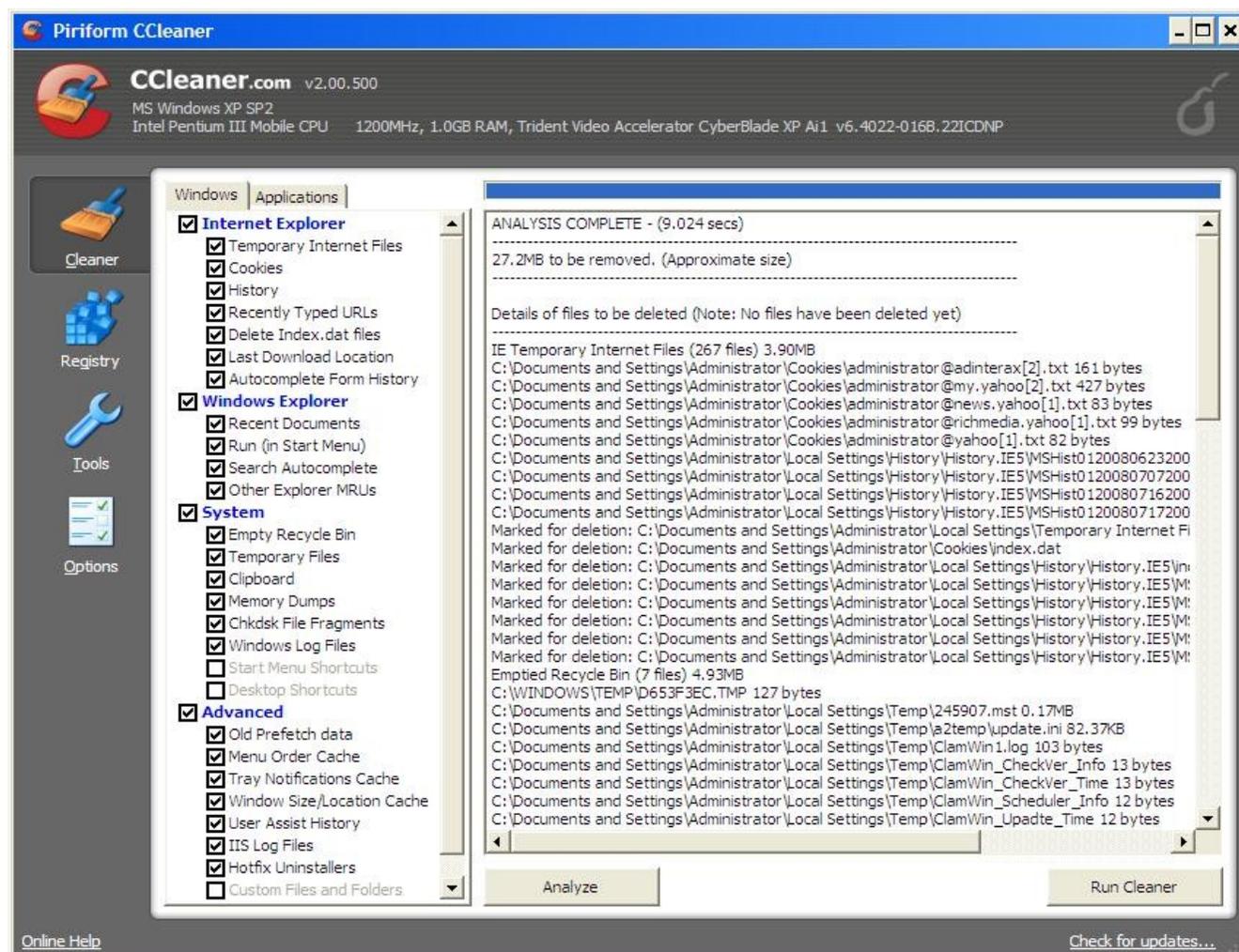
If you use Internet Explorer and have the default *Auto-Complete* feature turned on, your web surfing history is also kept in a second location -- in the Windows Registry. (You'll see web sites you've visited listed under the Registry key *TypedURLs*.)

If you turn off Auto-Complete, Internet Explorer no longer saves your web history in the Registry. To turn off Auto-complete, go into Internet Explorer, then select *Tools | Internet Options | Content | AutoComplete* and un-check the box for auto-complete of *Web addresses*.

Turning off Auto-Complete does **not** stop Windows from tracking your web site history in its **index.dat** files.

Several free programs securely erase your web site history from both the Registry and the **index.dat** files. Among them are [CCleaner](#), [Free Internet Windows Washer](#), [CleanUp!](#), and [ScrubXP](#). The shareware programs [PurgeIE](#) and [PurgeFox](#) are also popular. I've found [CCleaner](#) to be both thorough and easy-to-use.

Figure 9 – CCleaner protects your privacy by erasing web history, logs, cookies, temporary files, etc...



2.4 Windows Leaves Your Personal Information in its Temporary Files

Windows, web browsers, and other programs leave a ton of *temporary files* on your computer. Some hold web pages you've recently viewed, so that if you go back to that web page, you'll be able to view it quickly from disk instead of downloading it again from the web. Other files are used by Windows and its applications as temporary work areas. Still others are used to log program actions or store debugging information.

These temporary files sometimes contain personal information. For example, *web page caches* contain copies of web forms into which you've entered passwords or your credit card number. You may not wish to disclose the web pages, videos, images, audio files, and downloaded programs you've viewed lately.

The trouble is that these temporary files are **not** erased after use. Some remain until the system needs that disk space for another purpose. Others hang around forever, unless you know to clean them.

The free programs above that erase your web history also erase these temporary files and cache areas. [CCleaner](#) does a good job. Find more free programs [here](#) and a review of the best commercial programs [here](#).

2.5 Your “Most Recently Used” Lists Show What You’re Working On

Windows tracks the documents you’ve recently worked with through its *Most Recently Used* or [MRU lists](#).

MRU lists are kept by Microsoft Office products like Word and Excel, as well as applications from other vendors. Windows’s *Start | Documents* list also shows documents you have recently worked with.

Products keep MRU lists for your convenience. They help you recall and quickly open documents you’re currently working on.

These lists also offer the perfect tracking tool for anyone who wants to find out what you’ve been doing on your computer. They provide a ready-made behavioral profile. Windows and its applications keep many more MRU items than you might expect – thousands of them, if you have never cleared the lists.

Free program [MRU Blaster](#) cleans out these lists. Other free programs like [Ad-Aware Free](#), [CCleaner](#), and [Free Internet Windows Washer](#) erase many of the lists.

Run an MRU cleaner whenever you like. Remember that after you clean the lists, the “quick picks” of your recent documents will not appear in Word, Excel, or other products.

2.6 Product Registration Information May Be Hard to Change

When you register Windows, Microsoft Office, or other products, that information is stored in the Windows Registry. It can be read from there by any program or person who reads the Registry.

Registering a software product shows your legal ownership of the product and may be required to receive product support and updates. However, changing or eliminating the personal registration information later might be difficult. Some products have an *Options* or *User Information* panel in the program where you can easily change the product registration. But most require you to either directly edit the Windows Registry or even de-install the product to change or remove the personal registration data.

Consider carefully what you enter into any product’s registration panel when installing it. You may not be able to change it later. If you know you won’t need vendor support or updates and the product license permits it, you could enter blank registration information.

2.7 File “Properties” Expose Personal Data

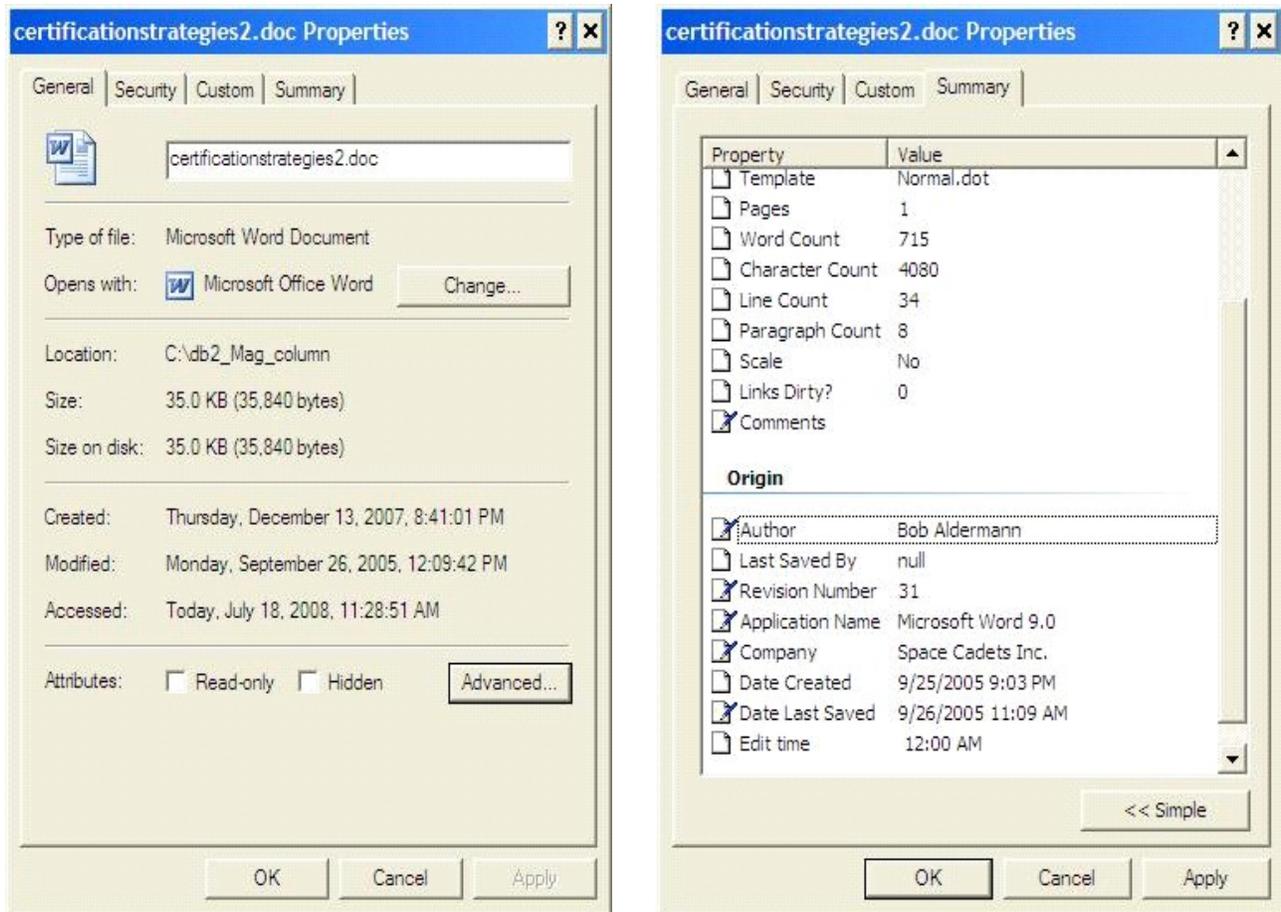
Right-click on any Microsoft Word, Excel, or Powerpoint file, and select *Properties* from the pop-up menu. You’ll see a tabbed set of panels that keep information about the file. (For some versions of Microsoft Office, you need to click the *Advanced* button to expose all the information.) You’ll see that Microsoft Office saves information about the file such as:

- Who created it
- The company at which it was created
- The name of the computer on which it was created
- A list of all who have edited it
- When it was created and when it was last saved
- The number of times it has been edited

- Total editing time
- Comments
- A hidden revision log
- Recent links used in the file
- Various statistics about the size of the file, the word count, etc

The information varies according to the type of file you view (Word, Excel, or Powerpoint) and the version of Microsoft Office that was used to create and edit the file. *You can't see everything Office saves in the Properties panel – some of it remains hidden from your view.*

Figure 10 – Here is some of the information exposed by Word's "File Properties" ...



You can change some of the *Properties* information by right-clicking on the file name, then editing it. Or alter it while editing the document by selecting *Edit | Properties*.

Other data is collected for you whether you want it or not, and you can not change it.

Should you care? It depends on whether it matters if anyone sees this information. In most cases it doesn't. But sometimes this data is private and its exposure matters.

Just ask former U.K. Prime Minister Tony Blair. He took Britain to war against Iraq in 2003 based on the contents of what he presented as his government's authoritative [Iraq Dossier](#). But [this Word file's properties](#) exposed the high-powered dossier as the work of an American graduate student, not a team of British

government experts. A political firestorm ensued.

Microsoft offers manual procedures [here](#) and [here](#) that minimize Office files' hidden information. But these are too cumbersome to be useful. Microsoft eventually developed a [free tool](#) to cleanse Office documents created with Office 2002 SP2 or later. But restrictions limit its value.

The free tool [Doc Scrubber](#) is an alternative for cleansing the *Properties metadata* from Word files.

Whichever tool you use, you must run it as your last action before you distribute your finished Office document.

Cleansing Microsoft Office files is inconvenient and it's difficult to remember to do it. Those who require "clean" office documents are advised to use the free office suite that competes with Office, called [OpenOffice.org](#).

The OpenOffice suite does not require personally-identifying Registration information and it gives you control over the *Properties* information. It reads and writes Microsoft Office file formats. (I edited this document interchangeably with OpenOffice and several different versions of Microsoft Word, then created the final PDF file using OpenOffice.) Read reviews of OpenOffice [here](#), [here](#), [here](#) and [here](#).

2.8 Microsoft Embeds Secret Identifiers in Your Documents

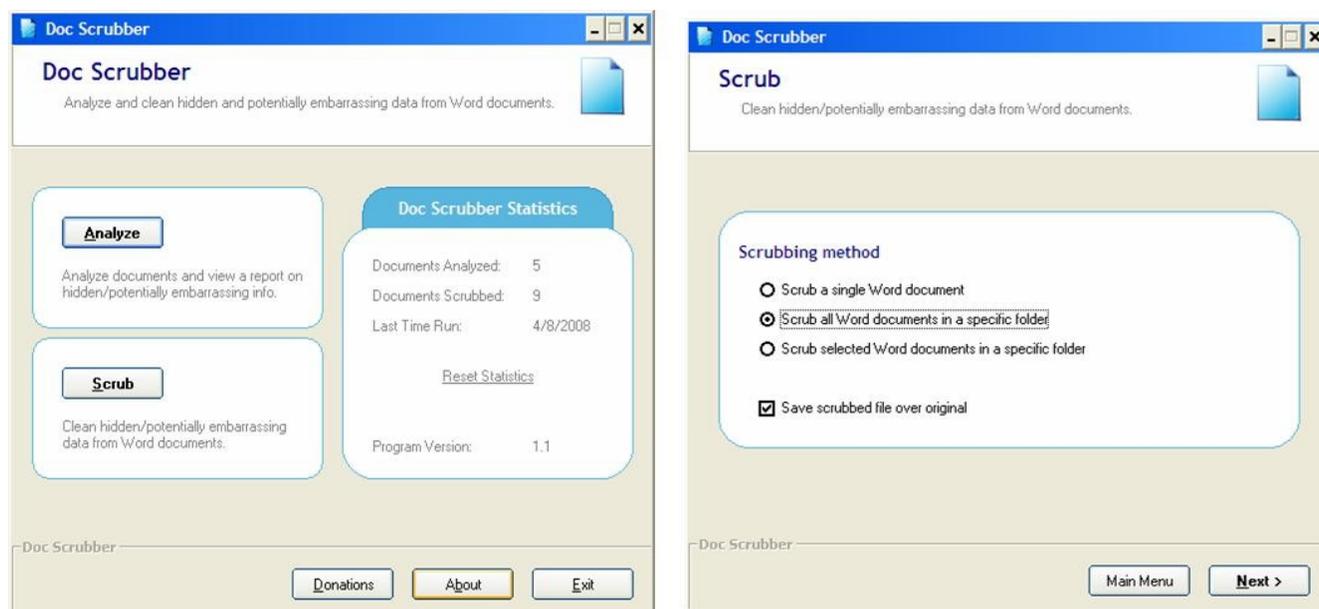
Windows, Windows Media Player, Internet Explorer, and other Microsoft applications contain a number that identifies the software called the [Globally Unique Identifier](#) or *GUID*.

Microsoft Office embeds the GUID in every document you create.

The GUID could be used to trace the documents you create back to your computer and copy of Microsoft Office. It could even theoretically be used to identify you when you surf the web.

The free program [ID-Blaster Plus](#) can randomize (change) the GUIDs embedded in Windows, Internet Explorer, and Windows Media player. The free program [Doc Scrubber](#) erases GUIDs contained in a single Word document or all the Word documents in a Folder.

Figure 11 – [Doc Scrubber](#) erases both personal "File Properties" data and GUIDs from Word files --



If you're concerned about secret identifiers embedded in your Office documents, use the [OpenOffice](#) suite instead. This compatible alternative to Microsoft Office doesn't embed GUIDs in your documents nor does it require personal registration and *Properties* information.

2.9 Windows Secretly Contacts Microsoft

Windows versions from XP on run Microsoft software components called [Windows Product Activation](#), [Windows Genuine Advantage](#), and [Office Genuine Advantage](#). The details of how these programs operate have changed over time, but their common element is that all "phone home" -- they silently contact remote Microsoft servers -- to periodically check that your copy of Microsoft software is licensed. If the software fails the check, penalties follow. These range from annoying messages, to reduced functionality, or even the inability to start Windows on your computer.

Concerns about this include:

- [False positives sometimes occur](#) or [Microsoft's servers are down and can't perform the check](#) (legal software is inaccurately flagged as illegal and [you pay the price](#))
- Privacy violation by [the information sent to Microsoft](#) (which uniquely identifies your computer and when you are using it)
- "Phoning home" raises security concerns
- Why does the software periodically send information about you to Microsoft when only one license check would suffice? Some consider [this software spyware](#). (Vista includes [several other new components](#) that gather data or send it to Microsoft.)

If Genuine Advantage concerns you, the article links in this section tell you everything you need to know. Google "disable WGA" and [you'll find many](#) more [how-to's](#) on this topic. You can install free tools like [RemoveWGA](#) or [xpy](#) to disable Windows' "phone home" function.

The article ["20+ Windows Vista Features and Services Harvest User Data for Microsoft"](#) argues that Microsoft is evolving Windows into a collection vehicle for data on your use of "your" system.

2.10 Chart of Microsoft's Tracking Technologies

I've discussed the major areas in which Windows and other Microsoft products track your computer use. In most cases you can not turn off this tracking. But the free programs I've described will delete the tracking information.

The chart below summarizes where and how Windows and other Microsoft products track your behavior. Some items apply only to specific software versions.

A few functions report your behavior back to Microsoft. Examples include when Windows Media Player [sent your personal audio and video play lists to Microsoft](#) and the company's attempts to use the Internet to remotely [cripple Windows installs it considers illegal](#).

--- Where Windows Tracks Your Behavior ---

Application Logs	Records on how often you run various programs
Clipboard Data	Data you've copied/pasted is in this memory area
Common Dialog History	Lists Windows "dialogs" with which you've interacted
Empty Directory Entries	File pointers unused by Windows but still usable by those with special software
Error Reporting Services	Reports Windows or Microsoft Office errors back to Microsoft
File Slack Space	"Unused" parts of file clusters on disk that may contain old data
File Properties	Office document <i>Properties</i> contain your personal editing information and more

Find/Search History	Lists all your Find or Search queries (used by Windows auto-complete)
GUIDs	Embedded secret codes that link Office documents back to your computer
Hotfix Uninstallers	Temporary files left for un-doing Windows updates
IIS Log files	Logged actions for Microsoft's IIS web server
Index.dat Files	Secret files that list all web sites you visit and other data
Infection reporting	Microsoft's Malicious Software Removal Tool reports infections to Microsoft
Last user login	Tracks the last user login to Windows
Microsoft Office History	MRU lists for Office products like Word, Excel, Powerpoint, Access, and Photo Editor
Office Genuine Advantage	Office phones home to Microsoft servers for license checks
Open/Save History	List of documents or files for these actions
Recently Opened Doc. List	MRU list accessible off <i>Start Documents</i>
Recycle Bin	Deleted files remain accessible here
Registration of MS Office	Registration information is kept in the product Options, Splash panels, and Registry
Registration for Windows	Registration information is kept in the Registry
Registry Backups	Registry backups may contain personal data you may have edited out of the Registry
Registry Fragment Files	Deleted or obsolete data in the Registry that remains there
Registry Streams	History of Explorer settings
Remote Help	Allows remote access to your computer for Help
Run History	Lists all programs you have run through Windows Run box
Scan Disk Files	Files output from SCANDISK (may contain valid data in *.chk files)
Start-Menu Click History	Dates and Times of all mouse clicks you make for the <i>Start Menu</i>
Start-Menu Order History	Records historical ordering of <i>Start Menu</i> items
Swap File	Parts of memory written to disk
Temporary Files	Temporary files used during program installation or execution
Time synchronization service	Synchronizes your computer clock by remote Internet verification
User Assist History	Most used programs on the <i>Start Menu</i>
Windows Authentication	Windows phones home to Microsoft servers for license checks
Windows log files	Trace results of Windows actions and installs
Windows Media Player content	Automatically downloads content-licenses through the Internet
Windows Media Player History	Lists the <i>Most Recently Used</i> (MRU) files for Windows Media Player
Windows Media Player metadata	Automatically retrieves metadata for audio CDs through the Internet
Windows Media Player Playlist	Your Windows Media Player play lists
Windows Media Player statistics	Sends your Windows Media Player usage statistics to Microsoft

--- Where Internet Explorer Tracks Your Behavior ---

Auto-complete form history	Everything you type into web site forms (inc. passwords & personal information)
Auto-complete for passwords	Convenient but less secure
Cookies	Data web sites store on your computer (sometimes used to track your surfing habits)
Downloaded files	Files you download while using the Internet
Favorites	Web sites you list as "favorites" in your browser
Plug-ins	Information saved or cached by third-party software that "plugs into" Internet Explorer
Searches	Searches are retained by both IE and search engines
Temporary files (<i>cache</i>)	Web pages the browser stores on disk
Web site error logs	Errors encountered during web site retrieval
Web sites visited	All the web sites you have ever visited are stored in the Registry and index.dat files

[This comparative review](#) rates ten commercial products versus many of the above functions.

2.11 Does Your Printer Spy on You?

Did you know that documents printed on your computer's printer [could be traced back to you](#)? This is the case if you use any of the color laser printers [on this list](#). The printers write a unique pattern on every page that can be traced back to your hardware. You can see these tiny dots with a magnifying glass.

The [United States government admitted](#) to prevailing upon printer manufacturers to include this capability and keep it secret from the public. If this concerns you, the best solution is to buy a printer that does not write its "fingerprint."

*Printer fingerprints are **not** a Windows issue.* They apply to any printer [on the list](#), regardless of whether the connected computer runs Windows, Apple's Mac OS, Linux, or some other operating system.

3. How to Protect Your Privacy When Using the Internet

[Privacy](#) is the ability to control when, how, and to whom your personal information is given. Privacy is power. Losing your privacy means losing personal power.

This section offers tips and technical advice to help you protect your privacy when using the Internet. It applies whether you use Windows or some other operating system, like Linux or Apple's Mac OS.

Web privacy is a fast-moving area in which technologies and laws are in flux. This guide can no more guarantee you absolute privacy than it can guarantee you a completely secure Windows. *But if you follow our tips you'll minimize your privacy exposure.*

3.1 Limit the Personal Information You Give Out

Before entering personal information into a web site form, a social network, or a forum, read the site's [Privacy Policy](#) and [Terms of Use](#). If they're legalistic and hard-to-read, chances are they have more to do with harvesting your personal data than protecting it.

Many agreements are written so that they can be changed at any time. This renders assurance of protection for your personal data worthless because the web site could simply change the agreement after you've provided the information. A few agreements even include fine print by which you agree to the installation of malware on your computer!

Few privacy policies guarantee that information will be destroyed as it ages. *Once given out, [information tends to live forever](#).* Few privacy policies give you any legal rights if your information is lost or stolen. In 2007 alone, [over 162 million](#) personal records were reported lost or stolen in the United States. (Yet it remains perfectly legal for companies to buy and sell your social security number and personal data.)

Once you post personal information on the web, you lose control over how that information is used. Changes to the "context" in which that data is used can harm you.

A classic example is the information students enter into social web sites like MySpace or Facebook for their friends' amusement, only to find it resurfacing later to harm their employment opportunities or their careers. Both sites [offer privacy controls that easily allow individuals to avoid such consequences](#) -- *but most users don't apply them.* People unknowingly assume risk they can not measure at the time they assume it.

The selling of personal data is a [largely-unregulated business](#) in the United States. It's a [multibillion dollar industry](#) called [information brokering](#). People who give out their personal data expose themselves to manipulation or harm.

Even the U.S. government is researching the harvesting of personal data from social networking sites for public surveillance. And why not? People voluntarily post the information.

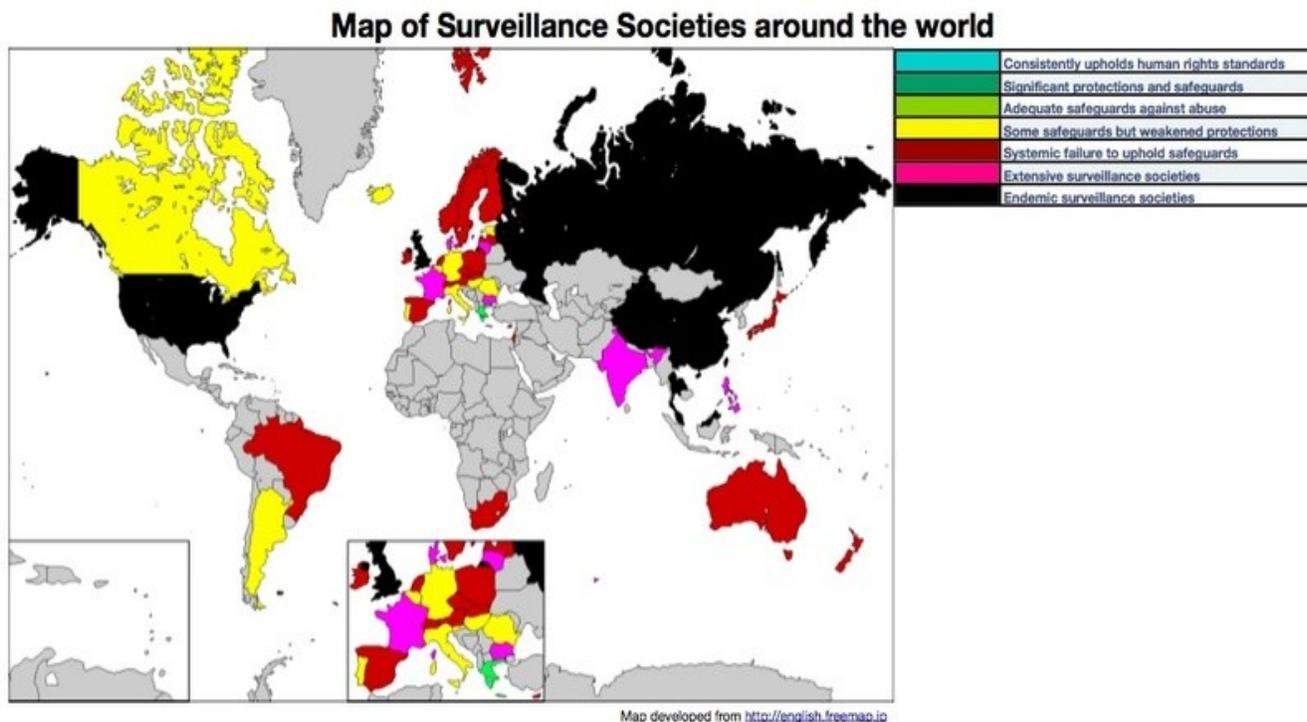
Fans of social networking will consider these cautions anachronistic. Please read how people expose themselves to manipulation or harm by posting personal data, found in authoritative books such as [The Digital Person](#), [The Soft Cage](#), or [The Future of Reputation: Gossip, Rumor and Privacy on the Internet](#).

We need legislation to assure minimal privacy rights for social network users, much the way we apply consumer-protection legislation to the credit card oligopoly. Meanwhile, protect yourself by educating yourself.

Tiny bits of information can be collected and compiled by web computers into comprehensive profiles. If a corporation or government can collect enough small bits of information – for example, just the names of all the web sites you visit – it can eventually develop a complete picture of who you are, what you do, how you live, and what you believe.

Privacy is power. You give away your personal power when you give out personal information.

Figure 12 – Think this discussion exaggerates? [Privacy International](#)'s rigorous, in-depth [study](#) ranks the United States as an “endemic surveillance society” ... right up there with China and Russia! ...



3.2 Don't Let Web Sites Track You

[Cookies](#) are small files that web sites store on your computer's disk. They allow web sites to store information about your interaction with them. For example, they might store the data required for you to purchase items across the several web pages this involves.

However, cookies – originally called *tracking cookies* – can also be used to track your movement across the web. Depending on the software using them, this data could be used to create a detailed record of your behavior as you surf. The resulting profile might be used for innocuous purposes, such as targeted marketing, or for malicious reasons, like spying.

Most browsers accept cookies by default. To retain your privacy, set the browser not to accept any cookies other than exceptions you specify. Then only web sites you approve can set cookies on your computer. A few web sites won't let you interact with them unless you accept their cookies -- but most will.

You can also set most browsers to automatically delete all cookies when you exit. This allows web sites to set the cookies required for transactions like purchasing through the web but prevents tracking you across sessions.

To manage cookie settings in your browser, access these panels --

To turn cookies on or off –

Internet Explorer	Tools Internet Options Privacy Advanced
Firefox (version 2 on)	Tools Options Privacy Cookies
Opera	Tools Quick Preferences Enable Cookies
K-Meleon	Tools Privacy Block Cookies
SeaMonkey	Edit Preferences Privacy & Security Cookies

To allow specific web sites to set cookies –

Internet Explorer	Tools Internet Options Privacy Edit
Firefox	Tools Options Privacy Cookies Exceptions
Opera	Tools Preferences Advanced Cookies Manage cookies
K-Meleon	Edit Preferences Privacy
SeaMonkey	Tools Cookie Manager

To “clear” (erase) all cookies currently on your computer for the specified browser –

Internet Explorer	Tools Internet Options General Delete Cookies
Firefox	Tools Clear Private Data
Opera	Tools Preferences Advanced Cookies
K-Meleon	Tools Privacy Clear Cookies
SeaMonkey	Tools Cookie Manager Manage Stored Cookies Remove All Cookies

To automatically clear all cookies whenever you exit the browser –

Internet Explorer	Not available
Firefox	Tools Options Privacy Cookies Settings...
Opera	Tools Preferences Advanced Cookies
K-Meleon	Tools Privacy Settings...
SeaMonkey	Not available

[CookieCentral](#) has more information about cookies and how to manage them. Other similar tracking mechanisms include [web bugs](#), [Flash cookies](#), [third-party local shared objects](#). These are less common than cookies and rather technical so follow the links and see the Appendix if they concern you.

3.3 Is Your Email Private?

Sending an email over the Internet is like sending a postcard through the mail. Anyone with the ability to intercept it can read it. *There is evidence that the United States government either scans or compiles data about every email sent in the country.*

You can keep the contents of your personal communications private by encrypting your email. [This web page](#) provides information and free downloads. It also lists programs that will encrypt your online interactive Chat. [This article](#) illustrates how to set up secure email step by step. [This article](#) tells how to encrypt email in Microsoft Office 2007.

Figure 13 – Download free email and chat encryption programs from [TheFreeCountry.org](http://www.thefreecountry.org) --



The trouble with encrypted email is that both the sender and the recipient must participate. It's impractical to send encrypted email to people you don't know. Or to anyone using a different encryption system.

The major email programs could easily support standardized, universally-compatible encryption in their clients -- but don't.

Remember that emails are often the basis for [phishing scams](#) – attempts to get you to reveal your personal information for nefarious purposes. Don't respond to email that may not be from a legitimate source. *Don't even open it.* Examples include claims you've won the lottery, pleas for help in handling large sums of money, sales pitches for outrageous deals, and the like.

Email may also be [spoofed](#) – masquerading as from a legitimate source when it is not. Examples are emails that ask you to click on a link to update your credit card account or those that ask for account information or passwords.

Legitimate businesses are well aware of criminal misuse of email and don't conduct serious business transactions through mass emailings!

Many people use two email addresses to avoid spam and retain their privacy. They use one account as a "junk" email address for filling out web site forms, joining forums, and the like. This email address doesn't disclose the

person's identity and it collects the spam. They reserve a second email account for personal communications. They never give this one out except to personal friends, so it remains spam-free.

3.4 Is Your Web Surfing Private?

If you tested your computer as suggested earlier using [ShieldsUp!](#), you saw that it gives out information to every web site you visit. This data includes your Internet protocol address, operating system, browser version, and more.

Your *Internet protocol address* or [IP address](#) is a unique identifier assigned to your computer when you access the Internet. Web sites can use it to track you. Your [Internet Service Provider](#) or *ISP* assigns your computer its IP address using one of several different techniques. How traceable you are on the web varies according to the technique your ISP employs along with several other factors, such as whether you allow web sites to set cookies and whether your computer is compromised by malware.

One way to mask who you are when web surfing is to change your IP address. [Anonymizing services](#) hide your IP address and location from the web sites you visit by stripping it out as your data passes through them on the way to your destination web site. Anonymizers help hide your identity and prevent web sites from tracking you but they are [not a perfect privacy solution](#) (because the anonymizer itself could be compromised).

[Anonymouse](#) is a very popular free anonymizing service. Find other free services [here](#) and [here](#).

A more robust approach to anonymity is offered by free software from [JAP](#) and [TOR](#). Both route your data through intermediary servers called [proxies](#) so that the destination web site can't identify you. Your data is encrypted in transit, so it can not be intercepted or read by anyone who [scans passing data](#).

Services like JAP and TOR present two downsides. First, your data is sent through intermediary computers on the way to its destination, so response time slows. Whether you still find it acceptable depends on many factors; the best way to find out is simply to try the software for yourself.

These systems still leave you exposed to privacy violations by your [Internet Service Provider](#). Your ISP is the your computer's entry sole point into the Internet, so your ISP can track all your online actions.

For this reason, when the Bush administration decided to monitor American citizens through the Internet, they proposed legislation that would force all ISPs to keep two years of data about all their customers' activities.

The government's current web surveillance program made it necessary for major ISPs like AT&T/Yahoo to change its privacy policy in June 2006 to say that AT&T – **not** its customers – *owns all the customers' Internet records and can use them however it likes*.

Repeated congressional proposals to immunize ISPs from all legal challenges only make sense if the ISPs colluded with the government in illegally monitoring Internet activities. The "FISA-II" law that finally passed in July 2008 prevents judicial investigation of illegal ISP and government surveillance, thereby permitting any such programs to continue without challenge.

Figure 14 – Web surf anonymously with Anonymouse.org or a similar service --



3.5 Are Your Web Searches Private?

Web sites that help you search the web are called [search engines](#). Popular search engines like Google, Yahoo!, and MSN Search retain records of all your web searches. Individually, the keywords you type into search engines show little. But aggregated, they may expose your identity. They may also expose your innermost thoughts – or be misinterpreted as doing so.

Here's an example. Say the search engine captures you entering this list of searches –

- kill wife
- how to kill wife
- killing with untraceable substance
- kill with unknown substance

Someone might interpret these searches as indicating that you should be reported to the authorities because you're planning a murder. But what if you were simply doing research for that murder mystery you always wanted to write? You can see need for search privacy. Do you have it?

The federal government has demanded search records from major search engines like Google, AOL, Yahoo, and MSN. While the government claims these requests are to combat sexual predators, most analysts believe they are for public surveillance and [data mining](#).

America Online (AOL) accidentally posted online 20 million personal queries from over 650,000 users. The data was immediately gobbled up and saved in other web servers. Although AOL apologized and quickly took down their posting, this data will probably remain available forever somewhere. [Some people can be identified by their “anonymous” searches](#) and have been harmed as a result of this violation of their privacy.

The AOL incident is a wake-up call to those who don't understand how small pieces of information about people can be collected by Internet servers, then compiled into revealing dossiers about our individual behaviors. This principle doesn't just apply to search engines. It extends to the web sites you visit, the books and products you buy online, the comments you enter into forums, the political web sites you read, and all your other web activities.

The AOL debacle demonstrates that web activities many assume to be anonymous can sometimes be traceable to specific individuals.

The [Electronic Frontier Foundation's](#) excellent white paper "[Six Tips to Protect Your Search Privacy](#)" offers these recommendations to ensure your search privacy --

- ❑ Don't include words in your searches that identify you personally (such as your name or social security number)
- ❑ Don't use your ISP's search engine (since they know who you are)
- ❑ Don't "log in" to search engine web sites
- ❑ Don't let the search engine set cookies
- ❑ Don't use the same IP address all the time
- ❑ Use anonymizers like [JAP](#) or [TOR](#) to thwart traceability

You can also use free search services like [Scroogle](#) that delete search histories after a couple days.

Figure 15 – Search the web without leaving a data trail through free services like [Scroogle.org](#) --



4. Wisdom

Your computer is your window into the vast, wonderful world of the Internet. Unfortunately it is also the window through which some corporations and governments monitor and track your behavior, and the portal through which malicious individuals and criminal gangs target you.

If you use Windows, Microsoft Office, and Internet Explorer, you need to be aware of how these products could compromise your security and privacy. Follow this guide's recommendations and you'll minimize your exposure.

Your privacy is not a design goal of Windows. It is up to you to make Windows secure and private.

Appendix: Further Information and Links

This appendix provides further information for each section of this guide. It includes links to other sources including articles and web sites.

You can download all the free software mentioned in this guide from these web sites --

- ❑ [The Free Country](#) (start [here](#))
- ❑ [Major Geeks](#) (start [here](#))
- ❑ [Download.com](#) (start [here](#))
- ❑ [Tech Support Alert](#) (gives recommendations on the best free software for every purpose)

Introduction

Security is the ability to keep your Windows system free of outside interference, while *privacy* is your ability to determine when, how, to who, and to what extent information about you is communicated.

[This article](#) and [this one](#) document how professional criminals have moved into penetrating Windows systems and how profitable this has become. [This web site](#) gives statistics on the exponential increase in malware.

This [New Yorker article](#) offers statistics on the increase in spam and other malware. Microsoft's own statistics profiling the kinds and occurrences of malware threats are summarized in [this Washington Post article](#) and also [here](#). [This forum discussion](#) links to several articles with statistics summarizing the costs and spread of computer malware. [This article](#) looks at the increasing threat from the corporate viewpoint.

1. How to Defend Against Penetration Attempts

1.1 Act Safely Online

Among the many good articles offering online safety tips are [this overview](#), [this introductory one from BBC](#), [this one at PCPitStop](#), and [this one for teens](#). David A. Wheeler's website has a nice comprehensive security how-to for home and small businesses [here](#).

1.2 Install Self-Defense Software

Overviews -- Find good introductions to the kinds of threats you face at the [PC Pitstop web site](#), the [SpywareInfo web site](#), and at [Road Runner Security and Abuse Control](#).

For those wanting technical details, [WindowsSecrets](#) consistently uncovers security and privacy vulnerabilities in Microsoft products, while [WindowsITPro](#) does a good job of analyzing flaws as they are found. [Security Convergence Journal](#) is useful from an operating-system neutral standpoint.

Firewall -- The Windows Vista, Windows XP SP2, and Windows XP / XP SP1 firewalls are all configured differently. To find which version of Windows you are running, right-click on *My Computer* and select *Properties*.

To configure the firewall for Windows Vista, see this Microsoft [article](#). The Vista firewall is "enabled" (turned on) by default, but its ability to stop rogue outbound data is off by default. You definitely want to enable this. [This article describes how](#).

To configure the firewall for Windows XP SP2, see this Microsoft [article](#). It also tells how the XP XSP2 firewall differs from the original XP and XP SP1 firewall, and briefly tells how to configure the original XP and XP SP1 firewalls.

To configure the firewall for Windows XP and Windows XP SP1, see this Microsoft [article](#). The firewall is "disabled" (turned off) by default. This is the original Windows firewall, which was called *Internet Connection Firewall (ICF)*.

"Every computer should run a firewall at all times when connected to the Internet" -- I have personally witnessed situations where corporate firewalls did not protect PCs, so I believe this statement applies even to computers within company firewalls and situations where you have a hardware firewall.

In an early release of this guide I mentioned that you can run two firewalls together without any harm. Readers have since written saying they have experienced situations where two firewalls conflicted so I dropped this statement.

You can rely on a *hardware firewall* (one that resides in your router) as an alternative to installing a *software firewall* on your computer. If you do, be sure to keep the firewall updated just the same as if it were installed on your computer.

Anti-Virus -- Read Wikipedia's [anti-virus page](#) and [TheFreeCountry's list and summary of free anti-virus programs](#) for a good understanding of viruses and how to protect against them.

Anti-Malware -- Here's Wikipedia's [overview article on malware](#). Read [TheFreeCountry's](#) descriptions of free anti-malware products [here](#) for a good idea of the threats out there and how to protect against them. [Here's](#) a good list of shareware programs for cleaning Windows. [This article](#) gives a good introduction to the growing threat posed by botnets.

Anti-Rootkit -- I debated whether to include this as a separate section, since the other anti-malware tools will protect most users adequately. Plus most anti-rootkit tools are either require a good bit of technical expertise to use or are still in beta at the time of writing. But ultimately this is an important threat area that is poised for growth so I decided a separate explanation is necessary.

[This InformationWeek article](#) reviews and compares six rootkit detectors, including both free and commercial products.

Intrusion Prevention -- See Wikipedia for [a good overview](#) and [TheFreeCountry's list and summaries](#) of free programs for a good understanding of this area.

1.3 Keep Your Programs Up-to-Date!

[Here are statistics](#) on how Windows users often don't patch important applications and why this is a problem.

[This Wikipedia article](#) gives good background on the evolution of Microsoft's automatic update facilities.

This [Microsoft article](#) describes Windows Update and Microsoft Update and their differences.

The original Windows Update web site is [here](#).

The [Microsoft Update Catalog](#) has a searchable interface and gives you more control over the update process.

[Here's a list of free alternatives](#) to Microsoft's Windows Update.

1.4 Test Your Computer's Defenses

[This commercial site](#) and [this Wikipedia article](#) offer good background on penetration testing.

There are several excellent security-testing programs I exclude here since they require expertise to use and interpret results. Among them are [Microsoft's Baseline Security Analyzer](#) (also downloadable from independent sites like File Hippo [here](#)) and the [Belarc Advisor](#).

1.5 Peer-to-Peer Programs Can Be Risky

For quick overviews of P2P dangers, read [this article](#), [this one](#), and [this](#).

[Here's a good overview at the Red Tape Chronicles](#).

[Here's a good article on P2P for parents](#) whose kids use the programs.

Here's [a quick corporate guide on P2P](#).

"The RIAA has sued over 20,000 people for file sharing as of July 2006" -- this figure comes from an [Electronic Frontier Foundation's](#) comprehensive [report on the subject](#).

1.6 Don't Let Another User Compromise Your Computer

I've personally seen cases of shared "family computers" where young people install games, P2P programs, and other "malware catchers," while the parents use the same computer for their banking and mutual fund accounts. ID theft resulted. If you cannot ensure that everyone who uses the computer conforms to the recommendations for safe surfing, don't use that computer for important personal data. One solution is to buy two computers. One will be the kids' game computer and the other a password-protected, data-encrypted parents' computer. I've even met individuals who have two computers, one for wild surfing, the other for their secure accounts (banking and online finance). A used Pentium III is perfectly adequate for surfing and general purpose software. They cost less than \$100.

1.7 Use Administrator Rights Sparingly

[This article](#) estimates that 70% to 80% of security threats can be thwarted by using accounts that do not have administrator rights. Some organizations enhance PC security by "locking down" user access and denying them use of administrator rights. This is not always welcomed by the users because they sometimes require administrator rights to do their jobs. Vista's *User Account Control* feature tries to resolve this controversy and satisfy the legitimate needs of both parties.

Read Microsoft's User Account Control guides [here](#) and [here](#). [This article](#) gives links to a core set of UAC articles from Microsoft and other sources. Vista's built-in Administrator user id does not have administrator rights until you enter your password, as prompted by UAC.

Windows consumer versions that pre-date Windows XP -- ME, 98, and 95 -- do not have administrator rights or the Administrator user id. All user ids effectively have "administrator rights" on these systems.

1.8 Use Strong Passwords

More advice on how to create good passwords can be found [here](#) and [here](#). [Here's what can happen](#) if you neglect to assign a password to

your router.

1.9 Always Back Up Your Data

Microsoft has several useful web pages on how to backup your data [here](#). [This site](#) offers plenty of good backup advice, free software, a discussion forum, and more.

If your computer won't start due to a software problem, there are many sources on the web to help. This Microsoft [article](#) helps resolve Vista startup problems, while [this one](#) covers how to create startup disks for all earlier Windows versions. If you need a boot disk for any version of Windows, [this site](#) provides them. This [article](#) tells about how to start Windows in [Safe Mode](#), which often works with computers that won't start otherwise.

1.10 Encrypt Your Data

Web pages on encryption tools at the [Free Country](#) and [Download.com](#) tell a lot more about this topic and offer many more free programs.

Data encryption techniques are complicated, as [this article](#) and [this one](#) in Wikipedia attest. I elected to keep this section simple and practical by avoiding the technical aspects of data encryption.

[Here](#) is an excellent series of articles on built-in encryption for Windows Vista and XP.

For volume-level encryption, the [Ultimate and Enterprise versions](#) of Vista provide a new feature called [BitLocker](#). [This article](#) tells you everything you need to know about it. [This article](#) and [this one](#) explore some of the advantages and downsides of BitLocker encryption. Given that it's presently restricted to the Ultimate and Enterprise versions of Vista, BitLocker is of little relevance to Windows desktop and laptop consumers.

1.11 Reduce Browser Vulnerabilities

Will Your Browser Run *Anybody's* Program? – I've simplified in saying browsers will run "any program" web sites push at them but this is a reasonable assumption for non-technical readers. I've also simplified by excluding discussion of the technologies involved and merely list the terms non-technical readers need to know to disable their browsers' programmability.

[Here's an ancient but easily understood explanation](#) of ActiveX and Java security issues that still has value even today.

Learn more about the uses and perils of *Active Scripting* [here](#) and [here](#), of *ActiveX* [here](#), [here](#), [here](#), and [here](#), and of *JavaScript* [here](#) and [here](#). Googling on these terms turns up many more explanations of security vulnerabilities from both the user and developer perspectives.

Internet Explorer Vulnerabilities – It is not my intent to disparage Internet Explorer -- this guide merely reflects consensus opinion in stating that the browser has historically been vulnerable to exploits. If you disagree please perform a web search on phrases like "Internet Explorer security defect" or "Internet Explorer insecurity" to read the evidence. Or visit the [Secunia web site](#), which publishes product security alerts and bug reports.

[This article](#) and [this one](#) describe the threat of [IE browser hijacking](#). Other exploits used against Internet Explorer include [code execution holes](#), [address bar spoofing](#), [multimedia component bugs](#), [cross-browser attacks](#), [encrypted code bypass](#), and others.

Sound computer science principles can be applied to address the security defects of traditional browser design. Examples include [virtual machines](#), the [browser appliance](#), and [sand-boxing](#). These are clearly superior methods to security than "browser-patching." But explaining them would be technical and they are not yet widely used on Windows computers, so they are out-of-scope to this guide.

1.12 Wireless Risks

[This web site](#) lists many articles on wireless security. [This article](#) at Microsoft tells you how to make an existing 802.11 B home network as secure as possible. *I strongly recommend upgrading any 802.11 B home network to 802.11 G.* See [this article](#), [this one](#), and [this one](#) for tips on setting up a secure home wireless network. Use [MAC address filtering](#) if your equipment supports it to limit access to your wireless network to specific computers. Some wireless routers ask you which encryption standard to use. From most desirable to least, here are the standards: AES/WPA2 -> WPA2 -> WPA -> 128-bit WEP -> 64-bit WEP -> 40-bit WEP. Any form of WEP security can easily be cracked by someone with the proper software and knowledge, so use AES, WPA, or WPA2 if available.

[Wikipedia](#) bluntly discloses the security risks of public hotspots. Public Wi-Fi is convenient but I wouldn't use it for online finances or other secure activities.

1.13 Replace Microsoft Software? (all links are in the text)

2. How Windows Tracks Your Behavior – and How to Stop It

2.1 How to Securely Delete Data

How to Securely Delete Files -- These programs will also securely delete [file slacks](#) or *cluster tip areas*, space near the end of files that might contain still-readable data, and *empty directory entries*, which might contain pointers to non-securely deleted files. Good secure-deletion programs also handle [swap space cleanup](#) and [alternate data streams \(ADS\)](#), two more ways in which data can be exposed. ADS only applies to computers running the NTFS file system (used since Windows XP and Windows 2000).

How to Securely Delete Email and Address Books – Read more about whether you can delete all your obsolete emails in organizational settings [here](#). Many organizations now keep *all* email ever sent due to the need to comply with the [Sarbanes-Oxley law](#).

How to Securely Delete All Personal Data on Your Computer – Even after reformatting a disk or running a secure erasure tool like [Darik's Boot and Nuke](#) it may be possible to recover data through very expensive “forensic analysis.” *If you have very high-value data and this is a concern for you, your best option is to run the disk secure-erasure tool -- then physically destroy the disk.*

2.2 The Registry Contains Personal Data

Good non-technical overviews of the Registry are at [ComputerHope](#) and [bleepingcomputer.com](#). PC Tools has [a good article](#) on how to alter Windows settings by *tweaking* the Registry.

For technical readers, Wikipedia has a [good overview of the Registry](#), as does [Microsoft](#).

If you edit your Registry, make a backup beforehand and be sure you know how to restore it. To edit Registry entry keys and their values, you access `Start | Run` and then enter the word **regedit** in the Run Box.

2.3 Windows Tracks All the Web Sites You've Ever Visited

I've simplified the details in this section to make the discussion accessible to non-technical readers.

There is third Registry location that may keep lists of web addresses. This is under the key hierarchy `Url History -> ZoneMap -> Domains`. *The web sites listed here are **not** ones you have visited!* They are kept in the Registry as part of Internet Explorer's *zoned domain security*. (See IE's zones by entering IE, then `Tools | Internet Options | Security`. The four icons represent four Internet security zones.)

The offensive web sites are placed there by anti-spyware products that restrict access to those web sites according to IE's security design. Find more on zoned security and how and why these web sites are in your Registry [here](#).

In addition to web sites visited, the **index.dat** files track recently-used files and documents, your search requests, and cookies.

2.4 Windows Leaves Your Personal Information in its Temporary Files

The best source of further information on these temporary files and cache areas are in the descriptions provided by the programs that clear them out. [This description of the commercial product Privacy Eraser Pro](#) gives a very complete idea of the kinds of information Windows and Internet Explorer leave on your hard drive.

2.5 Your “Most Recently Used” Lists Show What You're Doing

Here is [Microsoft's technical article on MRU lists](#).

2.6 Product Registration Information May Be Hard to Change

You can find whether entering a null product registration is permitted by reading the product license. Most products have a license file named either **license.txt** or **eula.txt** that describe the terms of product installation and support.

Free and open source products usually don't require registration from either a legal or functional standpoint. They offer big advantages if you're concerned about protecting your privacy.

2.7 File “Properties” Expose Personal Data

This discussion avoids minutiae about the *Properties* and hidden information Microsoft Office retains on documents as it all becomes very detailed. This paper is written for non-technical readers, and I believe the best advice for them is -- if this area concerns them -- to avoid the issue entirely by using [OpenOffice](#). Other free file-compatible Office replacements include [Abiword](#) for word processing and [Gnumeric](#) for spreadsheets.

The free *Remove Hidden Data Tool* from Microsoft has qualifications and limitations that are omitted in the interests of readability. Read [Microsoft's description](#) for more information.

Tips from an independent source on how to manage Office metadata are [here](#).

[This article published by Microsoft](#) gives their view of hidden information and offers useful background and tips.

2.8 Microsoft Embeds Secret Identifiers in Your Documents

Good introductions to GUIDs are at [Wikipedia](#) and [here](#). Microsoft's technical guide to how their software generates GUIDs is [here](#).

GUIDs were discovered in Microsoft products in 1999. The company hadn't told anyone about them previously. You can trace the controversy when the GUIDs were first discovered through [New York Times](#) articles such as [this one](#), [this](#), [this](#), [this](#), and [this](#). *In spite of all the controversy, Microsoft continues to embed GUIDs in all documents customers create -- without the informed consent of those customers.*

2.9 Windows Secretly Contacts Microsoft

[Wikipedia](#) entries tell the story: [Windows Product Activation](#), [Windows Genuine Advantage](#), and [Office Genuine Advantage](#). Vista-specific issues are discussed [here](#).

2.10 Chart of Microsoft's Tracking Technologies

I developed the chart of tracking technologies for Windows and Internet Explorer from information on the web sites of the vendors of cleansing tools (both free and commercial). The tools themselves also do a good job of listing what they cleanse in their program panels.

I've omitted from this paper the trap door [Microsoft embeds in Windows for the National Security Agency \(NSA\)](#) of the United States. It's considered proven that such an entry point exists, but its purpose and whether it has ever been used remain unknown.

2.11 Does Your Printer Spy on You?

The [Electronic Frontier Foundation](#) broke this story; their references in the text are considered authoritative.

3. How to Protect Your Privacy When Using the Internet

3.1 Limit the Personal Information You Give Out

MSNBC's excellent web site "[Privacy Lost](#)" offers highly readable articles on how privacy is being destroyed and why this matters.

I cite books in the text rather than web sites for those who want to learn about how "privacy is power" because the subject requires broad background. One can't understand the vast [data brokering](#) industry or the [implications of government surveillance](#) otherwise.

The [Privacy Rights Clearinghouse](#) compiles comprehensive statistics on [data breaches in the United States](#). (The figure of 162 million personal records being lost or stolen during 2007 is from that organization and is confirmed in [Time](#) magazine's December 31st 2007 issue.) Over 216 million personal records have been compromised over the past three years in the U.S.. It's incredible that it is still legal to buy and sell social security numbers in the U.S. and that this trade is unregulated.

[This article](#) alerts users to the dangers of "privacy" agreements. This guide takes a negative view of web and corporate Privacy Policies due to verifiable [corporate behavior](#).

[This article](#) tells how students are rethinking the costs of posting to MySpace and Facebook as they come to understand the public uses of "their" information. More about the downside of living an Internet social life is in "[Friends Don't Let Friends Post on MySpace: Posting on Networking Sites is Like a Tattoo -- but Worse.](#)" Read about how posting personal information can lead to job loss or career damage [here](#), [here](#) and [here](#). "[Say Everything](#)" postulates a generation gap between those under 25 and who post the most intimate details of their lives online, versus those who are older and resist giving out personal information.

[This article](#) illustrates how to (try to) protect your privacy when using MySpace, Facebook, and LinkedIn.

[This article](#) discusses how Facebook leverages your data through personalized [data aggregation](#).

Facebook is typical of many web sites in that its users give up rights to their data when posting it online. [Right at the top of their Privacy Policy page](#) Facebook says "**You should have control over your personal information.**" {boldface in original}. Yet the fine print of their Privacy Policy and Terms of Use directly contradicts this.

Facebook users grant Facebook an irrevocable, perpetual license to all of "their" content, plus they grant Facebook the rights to give that data to third parties and combine it with other data ---

From [Facebook's Terms of Use](#) (quoted from their web site in Nov 2007) -- "*By posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing.*"

From [Facebook's Privacy Policy](#) (quoted from their web site in Nov 2007) -- "*Facebook may also collect information about you*

from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (eg. photo tags) in order to provide you with more useful information and a more personalised experience. By using Facebook, you are consenting to have your personal data transferred to and processed in the United States."

And of course, Facebook adds -- "...We reserve the right to change our Privacy Policy and our Terms of Use at any time."

Social networking sites are like the "big three" credit card companies in that, while they are free-market corporations, there are a small group of them that provide a service fundamental to "normal life," as defined by those under in their twenties and teens. They should therefore be subject to federal privacy regulation in the same manner as the credit companies.

"Even the U.S. government is researching the harvesting of personal data from social networking sites for public surveillance."
-- More on how the U.S. government is working on incorporating social network profiles into their surveillance activities can be found [here](#), [here](#), [here](#), and [here](#).

3.2 Don't Let Web Sites Track You

I've simplified this discussion by leaving out cookie details like *first-party* versus *third-party*, *session* versus *cross-session*, whether the cookies include *personally-identifiable information*, etc.

[This Wikipedia article](#) defines cookies and describes other tracking technologies. [CookieCentral](#) gives background on cookies and advice on how to best manage them. [Here's an article on "How Web Server Cookies Threaten Your Privacy."](#)

Cookie-like tracking mechanisms include [web bugs](#), [Flash cookies](#), [third-party local shared objects](#), and other more esoteric tracking vehicles. I've left them out as they're a bit technical for this guide and are not as widely used.

3.3 Is Your Email Private?

"There is evidence that the United States government either scans or compiles data about every email sent in the country." – *Large-scale surveillance is possible because all traffic is digitized and passes through a limited number of master "trunk" switches, where it can be scanned.* The federal programs variously referred to as [Carnivore](#) or [Echelon](#) and [Total Information Awareness or Terrorist Information Awareness](#) keep changing their names but are appear to be alive and operating. Security expert [Bruce Schneier](#) offers good articles on current government surveillance programs, as do [Wired magazine's Threat Level web site](#), Glenn Greenwald at [Salon](#), and the [Raw Story](#).

[This article](#) describes the Congressional testimony of Mark Klein, a retired AT&T technician *who says he helped connect a device in 2003 that diverted and copied onto a government supercomputer every call, e-mail, and Internet site access on AT&T lines.* [This article](#) and [this one](#) detail Klein's claims. [Former National Security Agency analyst Russell Tice's](#) statements verify Klein's. [This article](#) describes the AT&T documents provided by Klein and concludes surveillance must be both domestic and comprehensive. [This article](#) asserts that the National Security Agency asked telecommunications companies for digital surveillance data seven months *prior* to the 9/11 attack.

[This article](#) and [this one](#) describe the several legislative attempts to secure immunity for telecommunications companies that gave private digital communications to the government illegally. [Proposing telecomm immunity](#) is itself the best proof of the *illegality of the government's domestic surveillance program.*

James Risen's many [New York Times](#) articles detail massive, illegal electronic domestic spying by the government. They have been collected into his book [State of War](#).

Along with Mr. Risen, [USA Today's articles](#) are generally credited with blowing the covers off the domestic surveillance story. President Bush called such disclosures "[disgraceful](#)" and [recommends prosecution of whistleblowers](#) through the [Espionage Act of 1917](#). He claims publicly the right to open anyone's U.S. mail without judicial oversight, directly contravening "settled law" on the question dating all the way back to the early 1800's. Perhaps the major email clients don't offer built-in universal, standardized encryption at government direction. [Here's a chronology of major articles](#) on the government's digital surveillance.

Find out about [PGP](#) and [S/MIME](#) encryption options for Outlook email [here](#). Find out more about Thunderbird email encryption [here](#).

Those who require the highest level of security in their communications might consider [steganography](#), hiding text within images. Download the free steganography program [ImageHide](#).

Two more tips for achieving the highest level of email safety – (1) turn off Outlook's email "Preview" feature, which automatically opens every email for you (2) turn off HTML rendering in email, which runs web page code on your computer.

3.4 Is Your Web Surfing Private?

[This chronology](#) tracks the key events of the government's web surveillance. [This article](#) tells how the Bush administration seeks to forestall public oversight of its web surveillance program through the state secrets doctrine. National Intelligence Director Mike McConnell [admitted to the existence of the illegal ISP-based surveillance program](#) in the same presentation to Congress in which he claimed that admitting its existence means that "some Americans are going to die."

Read about the Bush administration's proposals to force ISPs to keep two years of records for all their customers' Internet activities [here](#) and

[here](#). The congressional skirmish over these repeatedly-introduced proposals has been going on for several years. In July 2008 the “FISA-II” bill passed, giving telcomms retroactive immunity. The real import of this law is not that it shields telcomms from prosecution but rather that it prevents disclosure of illegalities and collusion by the federal government and the telcomms.

AT&T/Yahoo changed its “privacy” policy in mid-2006 to say that it owns all customer web use records and can do with them whatever it likes. Here’s a quote from the *AT&T Privacy Policy for AT&T Yahoo! and Video Services* dated June 23, 2006 –

“While your Account Information may be personal to you, these records constitute business records that are owned by AT&T... AT&T may disclose such records to protect its legitimate business interests, safeguard others, or respond to legal process.”

More on how AT&T asserts ownership of customers’ Internet data and what it means is [here](#), [here](#), [here](#), and [here](#).

Recognizing that a free society is incompatible with corporate tracking of web activities, [privacy advocates are recommending a “Do Not Track List,”](#) similar to the national “Do Not Call List” now maintained by the government for phone calls.

3.5 Are Your Web Searches Private?

Read [here](#) and [here](#) for overviews of search engine privacy issues. Find more tips on search engine privacy [here](#) and [here](#).

“The federal government has demanded search records from major search engines like Google, AOL, Yahoo, and MSN.” -- There have been many press articles on this topic and the twists and turns in events. For starters, see [here](#), [here](#), [here](#), [here](#) and [here](#). The Bush administration states it needs the search records to determine the amount of child pornography on the Internet, but as [commentators point out](#), that appears to be a red herring -- there are many more effective ways that could be determined. *Most analysts conclude this activity fits a pattern of citizen surveillance and data mining conducted by the federal government.*

More on the AOL debacle [here](#), [here](#), [here](#) and [here](#). The AOL scandal was a wake-up call to those who didn’t understand how compiling many small bits of information could ultimately identify and harm “anonymous” individuals. [“Why ‘Anonymous’ Data Sometimes Isn’t”](#) explores how little it takes to breach the supposed anonymity of *tracking data*.

4. Windows Wisdom

The goal of this paper is to help Windows users achieve greater security and privacy. It is intended to be objective and neutral towards vendors and products. This guide helps users better control their systems through increased understanding and downloading and installing free software tools.

It accepts as a given that the reader uses Windows, so it doesn’t discuss competing systems like Linux or Apple OS X. It tells users can they can replace parts of the Microsoft stack but discusses these decisions as tactical solutions, rather than as an overall strategy. For example, it mentions OpenOffice as a possible replacement for Microsoft Office, but strictly within the context of addressing Office’s privacy issues.

This guide does not discuss *why* Windows has security and privacy issues. There are important design and technical reasons but they fall outside the scope of this paper. Discussing them would only detract from the goal of helping Windows users achieve greater security and privacy.