



**THE CYBER-PRIVACY PRIMER:
Surfing the Web Without Surrendering Your Identity**

By

Edward Adams



GOLDEN KEY CAMPAIGN

TABLE OF CONTENTS

2	In Cyberspace Everyone Can Hear You Scream
3	The Cookie Monster
4	Anonymous Web-Surfing
5	Anonymous E-Mail
6	Other Anonymous Fixes and Tricks
7	On-Line Freebies to Hide Behind
8	Erased from History
9	Cleaning Up What's Already There
9	Advertising Your Web Site—Selectively
10	Betrayed by Your Computer
12	SHEL: Shredding, Hiding, Encrypting, Locking
13	Moves and Countermoves
14	Resources
16	Disclaimer

© 1998. All Rights Reserved.
Edward Adams
e-mail: cyberprimer@comports.com
<http://members.tripod.com/~cyberprimer/index.html>

Anonymity is a shield from the tyranny of the majority... It thus exemplifies the purposes behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.”
Justice Stevens, 1996.

IN CYBERSPACE EVERYONE CAN HEAR YOU SCREAM

Most people think of the Information Superhighway as a one-way street—a street they drive down to collect information, to buy things, or to just cruise around. But in cyberspace, when you reach out to grab something, something always grabs back at you. And it leaves you marked.

With each click of the mouse, you surrender a little piece of yourself, a little piece of your privacy. “Surfing the Net” is not an act of anonymity. You are broadcasting information about yourself, about your interests, about your on-line purchases, about your thoughts, about where you’ve been in cyberspace and what you saw and did there. It is a shock to most people to learn that they are leaving a trail as they wander through the Web.

The typical Web surfer is broadcasting at least this much information to anyone interested in collecting it:

- your name is _____ and you can be reached at _____@_____
- your computer is a PC running Windows 95 and your monitor is
- 800x600
- your Internet browser is Netscape
- your Internet service provider is _____ located in _____
- you just visited the _____ Web site
- we can access your news postings and Web pages

How does anyone know that? Check <http://www.anonymizer.com> to see what your computer is revealing about you. What else can someone learn about you? Plenty.

It was a shock to me too. Over the years my e-mail address has become the property of junk e-mailers. My comments and questions posted on electronic bulletin boards have been archived for everyone to read, and for one person to try suing me

over. My home page has been searched and catalogued by automatic robots or “spiders.” My residence and phone number are now available at a click. And if you need directions to my house, that’s just a click away too. In effect, the Internet has created a dossier on me. I never asked it to do that. I never knew it could do that. It can and it does. If you let it.

Should you care about your privacy while you’re clicking around the Web? That depends. Suppose you don’t want to be inundated with junk e-mail (“spam”) eating up your on-line time? Suppose you don’t want your favorite Web sites and purchases tracked by advertisers? Maybe you don’t want your employer building up a psychological profile of you based on your archived Internet messages. Maybe you’re a whistler-blower trying to avoid retaliation from your company, or you’re an abused spouse looking for help and information from on-line groups. Maybe you just don’t want people “flaming” you with abusive e-mail—and cc’ing your boss—over something you said on the Internet. These are legitimate reasons for wanting to protect your

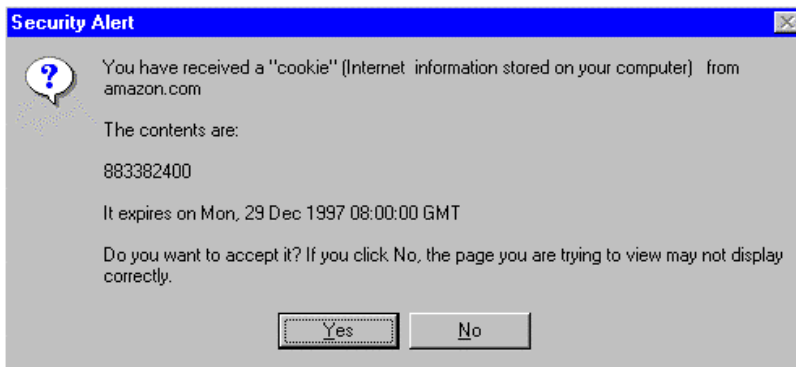
privacy and your identity.

According to the American Civil Liberties Union, 35% of companies spy on their employees by tracking their movements through the Web, and by intercepting computer files and e-mail messages. It is becoming increasingly easy to do; currently there are some two dozen software products on the market designed to track Internet use. Your company is probably already using some of these products. A white paper by CyberMedia notes that a third of Fortune 500 companies check medical records before hiring people. “Will they start checking Web surfing habits?”

Fortunately, there are a few simple precautions you can take to protect your privacy on the Net. This manual will show you how to begin guarding your on-line privacy. It doesn't take any more technical skill—or paranoia—than locking your car or using a smoke detector in your house. It's just a little more peace of mind in an age of a thousand Little Brothers watching us.

THE COOKIE MONSTER

Chances are, the minute you stepped into cyberspace, someone “tagged” you with a cookie. A cookie is a tiny text file that companies and Web servers insert into your browser files when you visit a Web site. Check your files; you're sure to find some. Clicking around the Web, it is almost impossible to avoid being stopped by one of these pop-up signs. If you've never seen one of these pop-up alerts, check your browser files. You're probably loaded with cookie files because your browser warning is set to OFF.



Why does someone want to tag your computer with a few lines of text? Well, for one thing, that tag can tell them how many times you've visited a Web site and what you did while you were there. If you looked at some pictures, read some articles, or bought something, they'll

know.

Cookies can also be secretly dropped into your browser by third party marketing companies. Here's one that was dropped into my browser: *id 1273585d doubleclick.net/ 0 1468938752 31583 4133902745696 29167724 **. These marketing companies track you around the Web and store information about your surfing and purchasing habits as a profile which they then sell to other companies and advertisers. To learn more about cookies visit Cookie Central on the Web. (Web site URLs are listed on page 22.)

Fortunately, there are a number of easy fixes to keep yourself from being profiled by marketers and tracked around the Web like a tagged bear.

ANONYMOUS WEB SURFING

The simplest thing to do is to surf the Web from an anonymous site. Some Web sites, for example, Anonymizer, Iproxy, and LPWA, allow you to be anonymous because they act as a barrier between your computer and the Web site you are visiting. You can see the Web site but it can't see you. And it can't give you a cookie.

Regular users of the Internet may want a more convenient fix than having to use a third party site to protect their privacy. A number of companies have developed software to protect you from being tagged and tracked.

One of the most convenient anti-cookie tools to use is Luckman's Anonymous Cookie for Internet Privacy. It is a free utility program that lets you disable all cookie files in your browser. Clicking on a small icon in the corner of your screen allows you to instantly switch between anonymous and true identity modes.

Other anti-cookie programs, such as Cookie Web Kit and Cookie Pal, are available from Cookie Central as freeware and shareware respectively. Most of these utilities let you automatically accept or reject cookies and delete those that have already been smuggled into your computer. These programs run under Windows 95. Some versions are available for the Mac.

The Privacy Software Corporation (PSC) sells inexpensive but sophisticated programs for Netscape and Internet Explorer browsers designed to help you regulate the flow of cookies. The PSC programs have additional features to provide you with an on-line alias, control over physical snooping into your computer, and control over accumulated browser files that you probably didn't even know you had. More about all that below.

For readers with experience in editing files, there are some permanent fixes you can make to your Netscape and Internet Explorer browsers to disable the cookie files and prevent anyone from giving you any new cookies. See Cookie Central for the technical details.

Of course, cookies are not entirely evil. They can perform useful tasks such as holding user IDs and passwords for accessing subscriber-based Web sites. They can also keep track of merchandise placed in on-line shopping baskets. The trick is to separate the good cookies from the bad cookies, and, thus, protect yourself from spammers and profilers.

Lucent Technologies (remember Bell Labs?) has come up with an interesting privacy experiment that relies on a proxy server and "target-revokable e-mail addresses." The Lucent Personalized Web Assistant (LPWA) is a proxy Web site service somewhat like Anonymizer and Iproxy in that it acts as a screen between you and another Web site. Lucent recently added the target-revokable e-mail addresses feature so users could automatically create and discard unique e-mail addresses for signing on to Web sites and posting to newsgroups.

When a site asks for a username, password, and e-mail address, Lucent instead supplies an alias-username, alias-password, and alias-e-mail address. Thus, you can surf the Net, register for information and access, and be recognized when you return to those sites. But your privacy, your real identity, is protected. Spammer bots or spiders that sift through Web sites and newsgroups looking for e-mail addresses will get your worthless alias instead.

Another form of Web anonymity is being tested by Lucent's parent, AT&T. It's called *Crowds*, (www.research.att.com/projects/crowds/) and it relies on creating anonymity by having users blend into crowds of other on-line users. *Crowds* uses a proxy server and the passing of one user's request through a random number of other users in a crowd. It's a novel approach, but it's hard to say how convenient it will turn out to be.

ANONYMOUS E-MAIL

Your e-mail address is a valuable piece of information. Advertisers want it. Bulk e-mailers ("spammers") want it. Nosy people and the occasional e-mail forger want it. You need to protect it. Here's how to start.

In your Internet browser, add an extra letter or number to your return e-mail address. For example, change *myname@connect.com* to *mynamex@connect.com*. Put your real address in the body of your e-mail message or as a part of your signature file. Or type something like *no_spam@yourserver.com*. This will prevent your address from being automatically harvested and used by bulk e-mailers and other spammers. It's also a popular way of telling people that you're hiding your e-mail address from junk e-mailers without suggesting that you're also trying to hide it from them.

Never respond to junk mail. If a junk mailer suggests that you to write back asking to be removed from a mailing list, don't. A response will only confirm that your address is valid and active, and therefore valuable for resale to other marketers. You'll keep getting spammed.

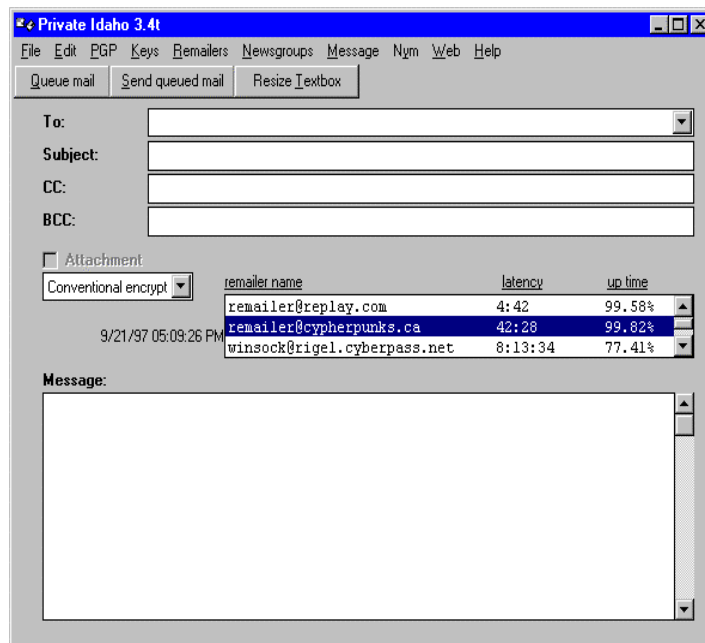
You can also sign up for anonymous e-mail accounts that will protect your identity and communications on the Web. Services such as CyberPass and Nymserver allow you to create fake IDs for sending and receiving e-mail. These services are particularly useful because you can post public messages to newsgroups and mailing lists—and receive responses—without anyone knowing your true identity¹.

Nym.alias.net is another anonymous remailer service. It's more complicated to use because it employs encryption for all of the e-mail traffic passing through its servers. It's also more secure—not even the administrators will know who you are—but you need to learn how to use the popular encryption software called Pretty Good Privacy (PGP). Once you get comfortable using some of the simpler remailer techniques you may want to step up to the greater security and sophistication of encrypted systems like PGP and the nym.alias.net service. PGP can also be employed with Juno e-mail (it's free) and a Windows-based remailer program that enables

you to engage in two-way anonymous e-mailing.

Another way to mask your identity is to use the wildly popular Private Idaho. PI is a Windows-based software system for remailing, posting to newsgroups, and encrypting e-mail messages. Private Idaho was designed by Joel McNamara. It's free and can be downloaded from a number of Internet sites, including McNamara's home page, <http://www.eskimo.com/~joelm/pi.html>.

PI is more secure because it also relies on PGP encryption. So again, it's a bit more complicated because you have to download it, set it up, and learn to use PGP. But if you spend a lot of time on-line and you're really interested in protecting your privacy, this system offers all of the tools and features you'll need to do that.



OTHER ANONYMOUS FIXES AND TRICKS

NSClean and IEClean software from PSC allow you to quickly switch back and forth between your real identity and a fake address (e.g., iamnot@here.net). Unlike CyberPass and Nymserver anonymous accounts, however, you cannot receive responses to these fake PSC e-mail addresses.

Rapid, anonymous e-mailing can also be done directly from some Internet sites. The Replay.com site, for example, has a Web interface (below) that allows you to paste in a message, and send it through a remailer before it reaches its intended recipient. The Anonymizer has a similar interface that let's you send anonymous e-mail.

Remailers are free services that mask your identity by stripping out your real e-mail

The screenshot shows a web-based email interface. At the top, there are two dropdown menus labeled 'Remailer 1' and 'Remailer 2'. Below these are input fields for 'To:' and 'Subject:'. To the right of the 'Subject' field are two buttons: 'reset' and 'send mail'. The main content area shows a preview of an email with the header 'Tuesday, February 10, 1998 - 20:01:52 MET' and the body text 'Don't forget to select a remailer!'.

address and any identifying message headers before forwarding the message to its recipient. Universities, Internet Service Providers (ISP) and private individuals run various remailer services—for various reasons. Some of the more popular and reliable remailers are listed below. All of them work by replacing your e-mail address with their own. For example, using *remailer@replay.com* to send an anonymous message, the recipient will see your address as *nobody@replay.com*. Some of these remailers also allow anonymous postings to newsgroups.

America On Line (AOL) is often referred to as the "largest anonymous remailer in the world." AOL gives each customer the option of selecting five different screen names that are traceable only by AOL and any lawmen and lawyers who come knocking at their doors. You can use those five different names to hide behind, then dump them, and create five more. In addition, it's easy to find free AOL disks offering hours of free on-line time. Sign on and start e-mailing and posting using a screen name. At the end of your free time, dump the disk, and pick up another one. As I write this, I have three free AOL disks in my office that were either mailed to me or were attached to computer magazines.

<u>Name</u>	<u>Remailer Address</u>
replay	remailer@replay.com
lcs	mix@anon.lcs.mit.edu
htp	mixer@htp.org
jam	remailer@cypherpunks.ca
cracker	remailer@anon.efga.org
squirrel	mix@squirrel.owl.de
magus	mix@magusnet.com
mix	mixmaster@remai.obscura.com
xenu	hendersn@zeta.org.au

ON-LINE FREEBIES TO HIDE BEHIND

As with AOL, you can use any number of free Internet-based e-mail services to set up an anonymous name and address. Bigfoot, HotMail, Net@ddress, and USAnet are just some of the free e-mail services available on-line. (Others are listed at the end.) It's easy to set up one of these Internet-based e-mail accounts. Use one for a while, then start up another one. They are convenient because you can send and receive e-mail from almost anywhere, including work, public libraries, and school. The point is, you don't have to be at home to send and receive e-mail. Unfortunately, you can't post to newsgroups from them.

The Lucent proxy server described on page 6 also provides a means of anonymously posting to newsgroups. Here's how. Sign on to the LPWA server and go to the newsgroup

database site, DejaNews.com or Reference.com. Sign in as a new member using the LPWA shortcuts and go to the newsgroup you want to post to. Write your post and send it. Because the LPWA server signs you up for permission to post using a random login and password, that is what will show up in the "From:" heading of your posted message. For example, if LPWA logs me into Reference.com as "UDEVQFpeUuMt02ce09d2@lpwa.com," that's who the anonymous post in the newsgroup will appear to have come from.

ERASED FROM HISTORY

Bulletin boards in the real world are useful because you can tack up a message for people to read and take it down later. When you remove it, it's pretty much gone for good. It's not that simple on the Web. Usually anything you write to a newsgroup, mailing list, or other discussion forum is going to be saved and archived. It will remain available to anyone and everyone for months or years. Maybe forever. DejaNews, one of the largest Internet databases for newsgroup messages, has archived messages dating back to 1995. They are planning to archive message traffic all the way back to 1979. On the Web, your words, your thoughts, will live on long after you've forgotten about them. But a quick search using your name or e-mail address can bring them all back. If that idea makes you uncomfortable you can prevent most archiving with the following utilities.

In the message header or at the beginning of your message to a newsgroup, type: *X-No-Archive: yes*. Skip a line and begin your message. This little tag will tell newsgroup databases like DejaNews, Alta Vista and Reference.Com not to save your message. Of course, your newsgroup post may continue to survive if other people copy it or reference it in their own posts. Still, it may be harder to search for later if it's buried in someone else's message under someone else's name. (*Reference.com* does not allow the *X-No-Archive* tag to be placed at the top of your message. All the more reason to post anonymously when using their site.)

You just posted an emotional, libelous message to a newsgroup. Can you pull it back before everyone has seen it? Maybe. Try sending a message to the newsgroup *control* and put *msg cancel <your message id number>* in the Subject line. The message number is in a header at the top of your posted message. You don't need anything in the message body. Be sure to send this cancel command from the same e-mail address you sent the earlier message from.

If you find that an embarrassing post of yours has already been archived for future posterity you can always try "nuking" it from the DejaNews Web site. Go to <http://www.dejanews.com/forms/nuke.shtml> and follow the directions. You have to "nuke" from the same e-mail account that you originally used to post your embarrassing message. This will eliminate it from DejaNews, but not from any other databases that also picked it up.

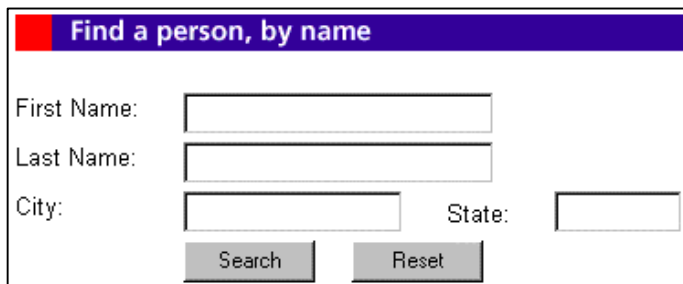
These tactics work pretty well for the larger archive databases. It's the smaller mailing lists and moderated forums that may present the greatest challenge to making your posts disappear. I have a feeling that a 1997 Internet question about technical tree climbing will follow me to the grave. It's not libelous or embarrassing; it has just become annoying to see it pop up

every time I do an Internet search on my name. You can always try asking the archive owner to delete your messages, but as one of them recently mentioned to me, "[it] wouldn't be much of an archive if I deleted info." Of course, it wouldn't be much of an archive if people stopped posting there. Touché!

CLEANING UP WHAT'S ALREADY THERE

OK. You're using remailers, throwaway e-mail addresses, anti-cookies software, and you're keeping your newsgroup posts from being collected and catalogued. You've taken some control of your on-line privacy. Now find out how much information about yourself was scooped up and stored on the Internet before you ever heard of the Internet. Use the Web's search engines to look for your name or e-mail address. The largest collectors and distributors of data (e.g., Alta Vista, Yahoo, Infoseek) are already listed under your browser search button. This is a good way to look for long-forgotten newsgroup postings that you'd like to nuke, and other information that might surprise you.

It's a good idea to check if your phone number and house address are available on-line. Internet directories like BigFoot, Four11, WhoWhere, The Big Book, and Switchboard make it easy to find people. Maybe too easy. You can search by name, e-mail address, city, and state. Some do reverse searches on phone numbers. Bigfoot is particularly "helpful" in providing maps right to your house. Frankly, everyone I want to have call or visit me knows how to do so. Everyone else, I don't want to see or hear from. No offense.



The image shows a web form with a purple header that says "Find a person, by name". Below the header are four input fields: "First Name:", "Last Name:", "City:", and "State:". There are two buttons at the bottom: "Search" and "Reset".

The best thing to do is visit each directory site and search on your name. (You'll probably also find all of your relatives.) If you hunt around these search sites you will usually find a page or form that allows you to request deletion/removal of your address and phone number. Use it.

Barring that you can usually find a page or form that allows you to modify or update your listing. Go to it and fill it with false information: fake address, fake phone number, wrong city. If you can't get off some of these lists the least you can do is make sure they list worthless information.

ADVERTISING YOUR WEB SITE...SELECTIVELY

The point of having a Web site or home page on the Internet is to have people visit it. You can advertise its presence by having it listed on the Web search engines mentioned above. When you register your URL (your home page address) with them they will send out little robot programs, called "spiders," to search your Web page and catalogue it's contents. These spiders search the entire home page, following all of your hypertext links, and eventually listing every page and every directory of your Web site. So a search of your name on HotBot, for example, is

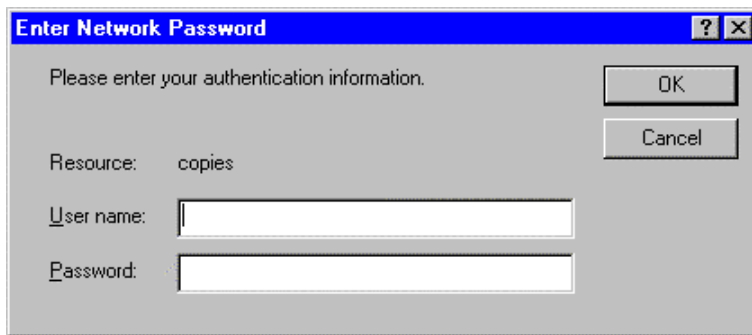
not going to list just your primary or index page, it's going to list every page associated with your site.

You may want to be selective about which pages you advertise and have catalogued for searches. To keep the spiders from crawling all over your pages add the following line of code in the body of every page that you don't wanted indexed:

<meta name="robots" content "noindex, nofollow">

This means the contents of that page won't be indexed and the hot links on that page won't be followed to your other pages. You probably have pages or pictures that the whole world doesn't really need to know about and probably doesn't want to know about. The *noindex, nofollow* tags will help to keep down the clutter on the Web. They also allow you to control the quantity of information about yourself being indexed on the Web.

To really protect parts of your Web site, you'll need to get password-protected pages. I have two password-protected pages: one contains my resume, the other contains pictures of my family. Try to see either page and this is what pops up:



I didn't see any need to advertise my complete work history to the world, but I wanted it available for potential employers and editors. I also didn't want pictures of my kids floating around either: especially when my address and a handy map to my house were available to anyone who wanted it.

Common sense—or a little paranoia—isn't necessarily a bad trait.

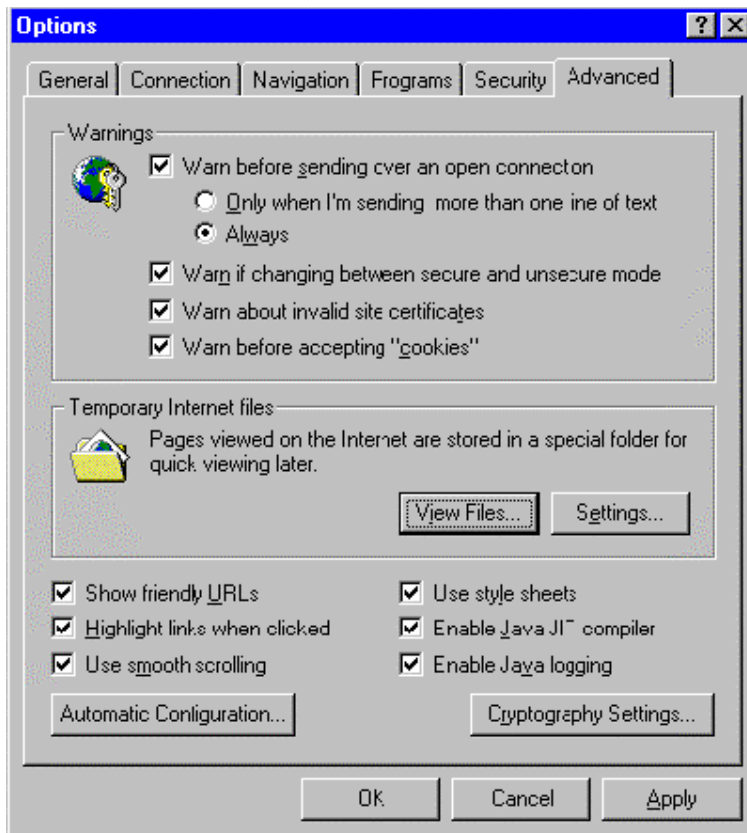
Your Internet Service Provider (ISP) can usually set up a password-protected page in just a few minutes. For those of you who would like to try it yourselves, see Joe Burns' site (<http://www.htmlgoodies.com/tutors/pw.html>) for some fairly straightforward instructions on how to do it. (It's a great site for other home page projects too.)

BETRAYED BY YOUR COMPUTER

Surprisingly, one of the biggest threats to your privacy is not the Web itself, but your own computer. It has the annoying habit of remember things. It also tends to create files that it doesn't tell you about. It remembers where you went on the Internet, for example, and it will tell anyone who asks. So don't let it. If you share a computer with someone at home, at work, or at school you'll leave a traceable record of your actions and interests on that machine. The next person who sits down in front of it can quickly discover what you've been doing all day. This is a

big problem at work where a little Web surfing or resume updating can get you into trouble. It could be a big problem at home too if your spouse discovers you've been spending a lot of time at the *alt.beer* newsgroup or the Playboy Web page.

The Netscape and Microsoft Internet Explorer browsers, in addition to storing cookie files, also keep track of everything on every Web site you visited. They are designed to do that so you can use your backward and forward browser buttons to jump to previously visited sites without having to wait for a fresh download. Browsers also list visited newsgroups and the newsgroup messages that you read, and the URL address window usually contains the last 10 or 20 sites you hit. But that same browser efficiency also lets someone else determine where you've been on the Web by looking through your browser and files.

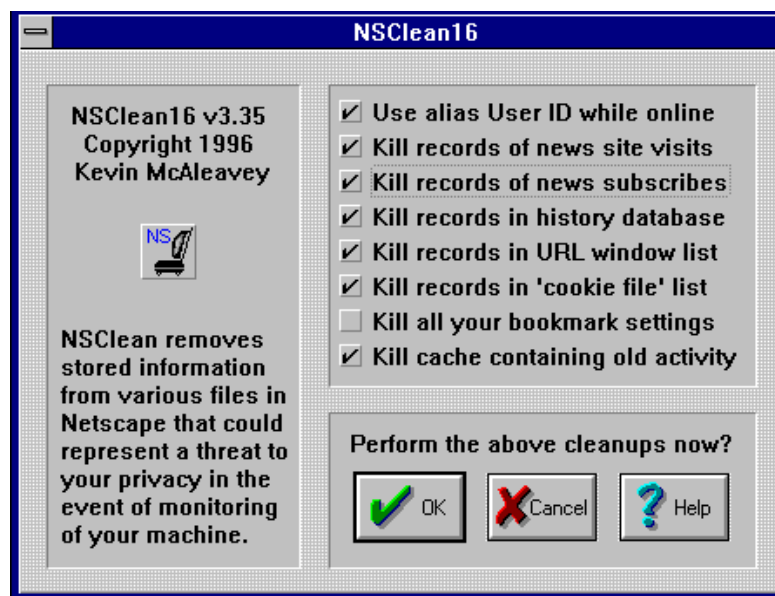


If you're incredibly disciplined, you can manually delete these trace files. Under Netscape's Preferences, click on "clear memory cache now" and "clear disk cache now" to delete the files that hold copies of the Web pages you visited. In File Manager, delete the *netscape.hst* files located in the Netscape directory and the Users subdirectory. As the developer of NSClean, Kevin McAleavey, notes, "Clearing out these files has no impact whatsoever on Netscape and there is seemingly no reason to keep these other than to possibly permit others to know what you do while you're on the net. [I] cannot fathom why such a file system exists or why such a detailed accounting of a user's on-line activities needs to be maintained."

In Microsoft Explorer (see the previous screen shot), click on Options, Advanced, Temporary Internet Files Settings, and hit Empty Folder. Make sure the amount of disk space allocated to this Internet junk is set to one percent, and that the box for "Warn before accepting "cookies"" is checked. Click Options again. Then click Navigation and the Clear History button.

Don't forget the browser bookmarks. If you bookmarked any Web sites, then anyone with access to your machine will know you've been to those sites. Decide what's safe to keep and delete the rest. And don't forget your e-mail files. Delete your drafts, your copies, and any received messages you don't want other people reading. Empty the e-mail trash files regularly.

Needless to say, remembering to make all of these deletions is a pain. Fortunately, software is available to take care of browser housekeeping. NSClean and IEClean, for example, can sanitize your respective Netscape and Explorer browser files with one click of the mouse. These programs also allow you to selectively eliminate all traces of visits to newsgroups and subscribed newsgroups; eliminate cookies; dump the cache; and kill all bookmarks. It's a pretty handy tool for a quick and total erasure of your Web activities.



Windows 95 also creates a little Windows directory called "Recent." It contains shortcuts to all of the files you recently worked on. If you've been updating your resume or writing love letters on company time the Recent directory may give you away. Delete its contents.

SHEL: SHREDDING, HIDING, ENCRYPTING, LOCKING

Obviously, you should employ a password to physically protect your computer from nosy people, and from accidental tampering by curious children. The problem with passwords is they're like weeds; they keep accumulating. Then you start to forget them. (I do anyway. I've got a page full of passwords and user IDs to dozens of files, Web sites, and databases.) A few companies are trying to take the pain out of password security by offering encrypted database systems to hold all of your passwords and user IDs. Password Manager for Windows 95 has such a database, plus automated access features for quick login and access to sites and files. Check shareware.com, download.com and ZDNet for similar programs.

There are also some very simple encryption programs you can download from the Web to encode sensitive files. I have a shareware copy of something called Crypt-o-Text from Savard Software that does a nice job of encoding files for storage or e-mailing. I'm sure the average

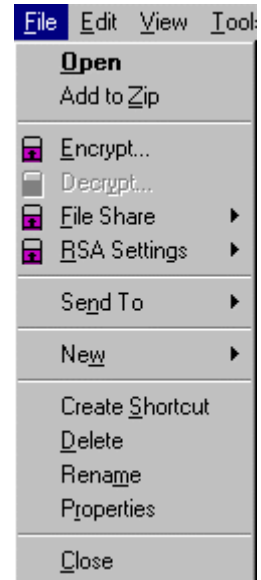
hacker or CIA electronics expert would laugh at some of these programs, but they're probably adequate for the average user concerned about his or her privacy. There are degrees of security and privacy, and there are degrees to which you need to go to protect that privacy.

Really serious encryption software based on secret- and public-key encryption algorithms is available from a number of sources. RSA, for example, provides SecurPC as freeware for Windows 95, 3.1x and Macs; RSA's higher end product, BSafe, is for sale. Using SecurPC, for example, you can e-mail encoded messages to people who do not have encryption software. A previously agreed upon password allows them to decrypt your message as a self-extracting file.

RSA products provide privacy, security and transaction authentication. The latter is particularly important if you plan to do a lot of on-line shopping with credit cards. Check your Microsoft and Netscape browser Help buttons for additional information about encryption and on-line security. The browser versions you use should support the Secure Socket Layers (SSL) protocol with 128-bit encryption. These standards will prevent your personnel information from being read by others as it is transmitted between your browser and a Web site.

You can also hide files and directories with programs like Magic Folders. Basically, it makes selected directories and their file contents invisible (more or less) so they can't be viewed, deleted, modified or run. Anyone checking your File Manager won't see any of these hidden files. Children pounding on the keyboard won't accidentally delete them either. Magic Folders is a shareware program.

Deleting files doesn't actually guarantee that they are gone forever. Surprise! Anyone with enough skill and incentive—your boss, maybe—can frequently recover deleted files. The only way to make files really disappear is to reformat your disks or your hard drive. The latter is a bit extreme so try using some recently developed software to "shred" your files. Shredder for Windows 95 and NT is a drag-and-drop system. It works by overwriting your files with an alternating pattern of bits. It then reduces the file size to 0 bytes, renames it, and finally deletes it. Not even your mother will be able to recover it.



MOVES AND COUNTERMOVES

When the newest version of Netscape Communicator was equipped with the ability to reject so-called "third party" cookies the cookie makers countered with a techno-dodge around Netscape's gatekeeper. Move and countermove. There's an intense little war going on in Cyberspace. Every move to protect privacy and free speech is eventually countered with a means to identify people and collect as much information about them as possible.

PointCast is an example of the coming "push" technology. Basically, it's an interactive screen saver that collects up-to-the-minute-information (news, weather, stock reports, etc.) and

displays it to the subscriber. You can customize the information: types of news stories, particular stocks, and the weather in certain cities. When my copy of PointCast crashed I was resigned to the fact that after I downloaded a new copy I would have to rebuild all of my personal options and settings. Wrong! PointCast had saved them all. They knew what my interests were, what stocks, what stories, what cities, and had them ready and waiting for me—or perhaps for someone else. This kind of technology is certainly useful because it 'pushes' self-selected information to you, but it also 'pulls' information from you. In this electronic tug-of-war who ultimately prevails?

And things will probably get worst. As Internet browsers become more fully integrated into a computer's operating systems the entire contents of your computer may become accessible to outsiders using clever new programs like ActiveX, Java and Javascript. Your files could become vulnerable to being copied, planted, deleted or altered. Your entire hard drive could be erased. Software is already being marketed to provide personal “firewalls” against hostile programs that might slip into your machine from the Web or from downloaded programs (so called Trojan Horse programs).

To prepare for this brave new on-line world, it is important to begin thinking now about your privacy and how best to protect it. Learn some of the basic methods described here. Start practicing with some of the tools currently available for guarding your privacy and ensuring your right to speak without fear of retaliation. Privacy, security in your own home, and freedom of expression are not gifts. They are won, and won back, every day. So start today.

To learn more about Internet privacy and anonymity visit some of the Web sites listed on the next page.

"Privacy is a right like any other. You have to exercise it or risk losing it." Philip Zimmermann

¹Technically, CyberPass and Nymserver are **pseudo**-anonymous remailers because the people running these remailers can—if they want to—read your mail and identify you. So don't try using pseudo-anonymous remailers to commit crimes or send death threats. Actually, don't try that from anywhere! There are truly anonymous remailers. They come in two flavors: cypherpunk and mixmaster. They're more private, but they're also harder to use. If you're interested in the technical distinctions between cypherpunk and mixmaster systems check some of the references listed at the end.

RESOURCES

Privacy-Related Web Sites

The Anonymizer	http://www.anonymizer.com
Cookie Central	http://www.cookiecentral.com
Cookie Tips	http://www.medsitenavigator.com/tips
Copyright Issues	http://www.clari.net/brad/copymyths.html
Crypto Resources	http://obscura.com/~loki/index.cgi
Download.com	http://www.download.com
Encryption	http://www.slaughterhouse.com/encrypt.html http://www.crypto.com/
Iproxy	http://www.iproxy.com
Junkmail	http://www.junkmail.org
PGP	http://www.pgp.com
Private Idaho	http://www.eskimo.com/~joelm/pi.html
Privacy Info	http://www.hacked.net
Privacy Software	http://www.nsclean.com
Privacy and Tools	http://www.hacked.net
Remailer FAQ	http://www.well.com/user/abacard/remail.html
Remailer List	http://www.publius.net/rlist.html
shareware.com	http://www.shareware.com
Spam	http://www.cauce.org
Web-based Remailer	http://www.myemail.net/anonymous.html
ZDNet	http://www.zdnet.com/swlib/

Books

The Computer Privacy Handbook : A Practical Guide to E-Mail Encryption, Data Protection, and PGP Privacy Software, by Andre Bacard, Peachpit Press, 1995.

The Official PGP User's Guide, by Philip R. Zimmermann, MIT Press, 1995.

Newsgroups

alt.privacy.anon-server

comp.society.privacy

Organizations

AAAS Project on Internet Anonymity,	http://www.aaas.org/spp/anon/
Center for Democracy and Technology,	http://www.cdt.org
Electronic Frontier Foundation,	http://www.eff.org
Electronic Privacy Information Center,	http://www.epic.org
Internet Privacy Coalition,	http://www.privacy.org/ipc/

DISCLAIMER

I have no financial interest in any of the products, companies or Web sites mentioned above. Any products or services, free or otherwise, which I have mentioned or highlighted, was done so to illustrate a point, not to make an endorsement. Readers are encouraged to try different applications and technologies, and to make use of those they find most appropriate for their particular needs.