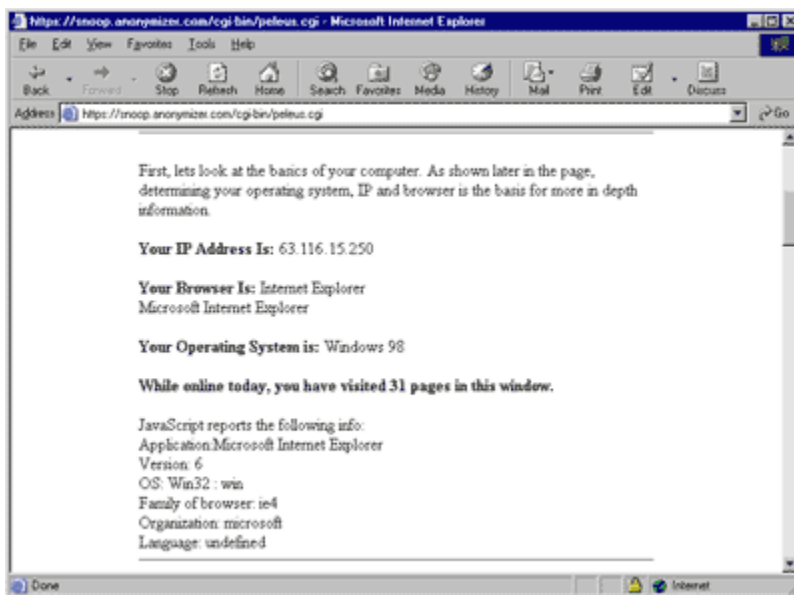


Protect your personal information from Internet Peeping Toms

by Boris Loza, PhD, CISSP
Tego System Inc

You'd probably be surprised if you knew what information about yourself is available on the Internet! Do you want to know what kind of information? Go to <http://www.leader.ru/secure/who.html> or <http://snoop.anonymizer.com> and check it out. If you can't wait, look at **Figure A** for a sample.

Figure A: *Internet security sites can show you what kind of information other sites are capable of collecting from you.*



As you see, they can find out where you've come from (your IP address and domain name), your operating system (Windows 98), browser (Internet Explorer 6), and many other things. Besides this, many servers keep careful records of the information you enter into search engines, information that you submit in online forms, your online shopping habits, and information about files you've uploaded or downloaded. In this article, we'll show what you can do to minimize, and sometimes prevent, your computer from submitting information to the Internet on your behalf.

Private eyes are watching you

Web administrators have plenty of tricks up their sleeves when it comes to gathering personal information about you, your system and your surfing habits. Fortunately, you have just as many methods at your disposal for cutting them off at the pass. We'll begin our overview of privacy theft patterns and prevention by offering you a brief taste of the technologies that sneaky administrators and advertisers are using. Then we'll get into deeper detail about the functions of cookies, Web bugs, proxy servers and remailers, including various techniques you can use to turn the tables on unwelcome spy tacticians. Finally, we'll wrap up with some tips you can put to use for keeping your system free of footprints that you'd prefer not to leave behind you as you surf the Internet.

Who gets this information and how?

Some companies, such as DoubleClick, create large databases of such information, which are used by target advertising companies or can be sold to any interested buyers. Have you ever wondered why every copy of Netscape Navigator running on Microsoft Windows defaults to <http://www.netscape.com> as a home page and Internet Explorer browser defaults to <http://www.msn.com>? There's a reason!

Another method that Web sites use to track visitors is a special file called a cookie, which contains a small amount of information transmitted between a Web server and a browser. Cookies can contain your username/ID, computer type, IP address and server location.

In the June 2001 issue's Internet Savant column, we told you about Web bugs, also known as clear GIFs. Like cookies, Web bugs are electronic tags that help Web sites and advertisers track visitors' whereabouts in cyberspace. The placement of a Web bug on a page allows the site hosting the banner ad to know your IP address and the page that you visited. This can be further correlated to cookie information that may be sent by your browser as part of the request to retrieve the page. But Web bugs are invisible on the page and are much smaller, about the size of the period at the end of this sentence. Unlike cookies, people can't see Web bugs, and anti-cookie filters won't catch them.

Browsers also contain other useful data for those who know how to make use of it, such as hit logging and GUID numbers, as used by Microsoft's Internet Explorer. Hit logging keeps track of all of your online activities. When you click on a banner ad, a record is made of how long you looked at it and what ad you clicked on, as well as personal information stored by the IE browser. Hit logging is also designed to 'phone home' to the server that created it.

GUID numbers are randomly generated "Guaranteed Unique" or "Globally Unique" ID numbers. It's highly unlikely that these numbers will ever occur twice across the planet. They're the ultimate "electronic dog tag" and can survive even if you kill the cookies and remove the spyware. Since the GUID number is kept on your system, it can be requested at any time. And since the GUID's creator has it on its databases—along with your name, address and other registration details—the potential for creating a system that tracks your every online move is enormous. By the way, GUID helped to capture a creator of the Melissa virus, but that's another story.

Many of the applications that you use and the companies you come in contact with every day use spyware and "phone home" technology to learn more about your system configuration, surfing habits and demographic information. Companies collect this information in order to determine the best way to target banner and pop-up advertisements. In most cases, this type of information isn't intended to be harmful. However, if the thought of it happening without your consent makes you uncomfortable, then you reserve the right to do everything you can to prevent it from happening. Now let's begin reviewing what you can do to protect yourself and your system from unwanted Internet spies.

The recipe for cookies

When you revisit an Internet server, your browser shares the cookie previously installed on your hard drive, providing information that quickly identifies you. Whenever you hit a Web site supported by advertising, the ad server reads the cookie from your machine. The ad server then uses your cookie to look up your profile and determine which ad to serve to you dynamically, based on the interests it's gleaned from your surfing activities at its member sites. The ad server also records which advertisements you've clicked through. The type of ad and the amount of time you've spent at the site is also captured. Also keep in mind that cookies, the subject of several lawsuits, are sent in clear text, in both directions, whenever encryption isn't used.

You can view your system's cookie content by opening any of the TXT files in the Windows\Cookies folder if you're using Internet Explorer or by opening the cookies.txt file in your user folder if you're a Netscape Navigator user. These files consist of a block of ASCII text. Briefly, the types of information tidbits you'll find within these files is the URL by whom and for which the cookie was created, the

name of the ID that the cookie is designed to work with, your IP address, the cookie's expiration date, and its value.

The easiest way to protect yourself from cookies is to disable this feature by choosing Tools > Internet Options from the menu bar and clicking on the Security tab if you're using Internet Explorer or by choosing Edit > Preferences > Advanced from the menu bar if you're using Netscape Navigator. Here (and on the Privacy tab in IE 6), you can increase or customize your security level to block or prompt for cookie acceptance on a site-by-site basis. However, some Web sites (such as <http://www.hotmail.com>) require cookies. If you're using Netscape Navigator, you can fool such Web sites by deleting the contents of the cookies file and replacing them with a link to /dev/null (works for UNIX users only):

```
ln -s /dev/null cookies
```

In this scenario, all cookies are accepted, but no information is stored on your hard drive.

Anatomy of a Web bug

Web bugs, like cookies, are usually used for tracking customer habits but are much harder to detect. Although Web bugs are designed to monitor who's reading a Web page or email message, they stand the potential to be used toward malicious ends, such as grabbing IP addresses or installing files. The security company Security Space, in a monthly report (<http://www.securityspace.com%2fsurvey%2fdata%2fman.200105%2fwebbug.html>), has identified companies that benefit from the use of Web bugs, including online advertising networks DoubleClick and LinkExchange, as well as Yahoo! and America Online. For more information about tracking down Web bugs, see the June 2001 Internet Savant column, titled "Web bugs." Or rather than trying to search them out yourself, you can download Privacy Foundation's Bugnosis Web bug detection utility for Internet Explorer at <http://www.bugnosis.org>.

Web bugs used with emails allow the measurement of how many people have viewed the same email message in a marketing campaign. They help to detect whether someone has viewed a message. (People who don't view a message are removed from the list for future mailings.) They also help to synchronize a Web browser cookie to a particular email address, allowing a Web site to know the identity of people who come to the site at a later date.

For a demonstration of a bugged Yahoo profile, see <http://profiles.yahoo.com/webbug2000>. This profile contains a visible Web bug image that's being loaded from a server other than Yahoo. The Web bug provides a log of everyone who has visited the profile page. For more information, check The Web Bug FAQ at http://www.eff.org%2fpub%2fPrivacy%2fProfiling_cookies_webbugs%2fweb_bug.html.

Proxies and anonymity servers

As we mentioned in the October 2001 article "Surf the Net without leaving a trace," one can remain anonymous while Web surfing by using a proxy server. A proxy acts as an intermediary, routing communications between clients and the rest of a network. Web proxies can hide your IP address and allow you to stay anonymous. If you aren't currently using a proxy server, you can choose one from the Free Proxy Public Servers List at <http://tools.rosinstrument.com/proxy>.

To configure Internet Explorer to use a proxy server, choose Tools > Internet Options from the menu bar and then click on the Connections tab. Click the LAN Settings button, and then select the Use A Proxy Server check box. Enter the proxy server's address and port number in the corresponding text boxes, and then click OK to close the LAN Settings and Internet Options dialog boxes. If you're using Netscape Navigator, choose Edit > Preferences from the menu bar and then navigate to the Advanced > Proxies category. Select the Manual Proxy Configuration option button, and then click the View button. In the resulting dialog box, enter the host name of the proxy you're going to use and a port number (provided by proxy server). When you've finished, click OK to close this and the Preferences dialog boxes.

To check whether your proxy server reveals your IP address, go to <http://www.all-nettools.com/pr.htm>. If you get the message Proxy server is detected!, then there's a security hole in your proxy, and information about your real IP address is listed. (In this case, try to use another proxy.) If the message is Proxy server is not detected, everything should be okay.

If you don't want to use a proxy server, try one of the Anonymity Providing Servers listed in **Table A**. These servers act as a proxy, since Web pages are retrieved by them rather than by the person actually browsing the Web (you). Go to one of these Web sites and just type a URL you want to visit—the server does the job for you, securing you from many potential dangers. SafeWeb uses 128-bit SSL encryption for all HTTP data, which prevents your ISP from tracking your Internet activities. The only traces that are left from your browsing are in your browser's history list. For more information about anonymity sites and software, as well as links to additional products and services worth trying, be sure to check out our October 2001 article.

Table A: Anonymity servers	
Name	URL
Servers with SSL support	
SafeWeb	http://www.safeweb.com
Rewebber	http://www.rewebber.de and www.anon.de
Servers without SSL support	
Anonymouse	http://http://anonymouse.is4u.de
Aixs NET	http://www.aixs.net
SiegeSoft	http://www.siegesoft.com
Orangatango	http://http:%2f%2forangatango.com%2fhome%2findex.ie.html

Remailers

If you want to remain anonymous while sending emails, you can use a remailer. This is a special service that receives an email message from you, then readdresses it and sends it to the person you want to send it to. During the process, any headers that might point back to you are removed. Many remailers are available on the Internet; some of them let you enter a fake return address, but most of them directly state that the message is sent from an anonymous source. For a list of remailers worth checking out, visit <http://security.tao.ca/email.shtml>.

Other useful tips

Banner ads can be a nuisance and can also give third parties another method to track your Web use. Fortunately, there are many ad-blocking software products available on the Internet that can help you suppress banner ads and pop-up ads from displaying during your surfing sessions. We'll take a closer look at these types of products in a future article.

You may also want to clear out or limit your browser's history list. This is something that should be done each time you're finished with your browsing, if you don't want someone who has access to your computer to be able to easily see where you've been surfing. If you're using Internet Explorer, choose Tools > Internet Options from the menu bar and then click on the General tab (if necessary). You can prevent IE from saving any sites to your History list by changing the Days To Keep Pages In History setting to 0. You can clear your current History list by clicking the Clear History button. If you use Netscape on UNIX, you can easily clear your history by deleting the ~/.netscape/history.* files at the end of your session.

Another place that your Web trail is recorded is the cache directory—a temporary storage area for recently visited pages and images. The cache allows for repeatedly visited Web sites to show up more quickly when you reload them into your browser. If you don't want people to read your cache files, they should be deleted. Note, however, that on slower machines with slow connections, this will result in a noticeable decrease in the speed when your computer brings up previously visited Web pages. To delete your cache in Internet Explorer, access the General property sheet as we explained earlier, click the Delete Files button in the Temporary Internet Files panel, and then click OK. You can decrease the amount of disk space reserved for cached files by clicking the Settings button and decreasing the Amount Of Disk Space To Use setting. If you're using Netscape Navigator, select Edit > Preferences from the menu bar and navigate to the Advanced > Cache category, then click the Clear Disk Cache button and click OK. To lower the disk space reserved for cached files, change the Disk Cache setting as appropriate.