Whenever you surf the Web, you leave yourself open to being snooped upon by web sites. They can track your online travels, know what operating system and browser you’re running, find out your machine name, peer into your clipboard, uncover the last sites you’ve visited, examine your history list, delve into your cache, examine your IP address and use that to learn basic information about you such as your geographic location, and more. To a great extent, your Internet life is an open book when you visit.

Don’t believe me? Head to http://www.anonymizer.com/privacytest/. This page, run by the Anonymizer.com web service, tells you your IP address and machine name. And that’s just a start. Click the links such as Exposed Clipboard and Geographical Location. You’ll see just a small sampling of what web sites can learn about you. Figure 4-12 shows a web site reporting on my IP address, the contents of my clipboard, my browser information, and my geographic location. It’s close enough; I live in Cambridge rather than Boston, and we generally require that people turn over their passports at the border.

Much of the reason why web sites can find out this information about you is due to the trusting nature of the Internet’s infrastructure and is inherent in the open client/server relationship between your web browser and the servers on the sites you visit. But a lot of it also has to do with the ability to match up information from your PC to information in publicly available databases—for example, databases that have information about IP addresses.

The best way to make sure web sites can’t gather personal information about you and your computer is to surf anonymously; use an anonymous proxy server to sit between you and the web sites you visit. When you use an anonymous proxy server, your browser doesn’t contact a web site directly. Instead, it tells a proxy server which web site you want to visit. The proxy server then contacts the web site, and when you get the web site’s page you don’t get it directly from the site. Instead, it’s delivered to you by the proxy server. In that way, your browser never directly contacts the web server whose site you want to view. The web site sees the IP address of the proxy server, not your PC’s IP address. It can’t read your cookies, see your history list, or examine your clipboard and cache because your PC is never in direct contact with it. You’re able to surf anonymously, without a trace.
Figure 4-12. The Anonymizer.com web service, exposing my current geographic location
There are two primary ways to use anonymous proxy servers. You can run client software on your PC, which does the work of contacting the server for you, or you can visit a web site, which does the work of contacting the server.

**Web-Based Anonymizer**

If you don’t want to go to the hassle of installing a client—and if you don’t want to pay for software—to surf anonymously, go to Anonymizer.com (http://www.anonymizer.com). In the box near the top of the page, type the name of the site to which you want to surf, and you’ll head there anonymously. The proxy server will grab the page for you, and you’ll get the page from the proxy server. You can also download a free version that runs as a toolbar in Internet Explorer. Surf as you would normally, and you’ll visit those web sites directly. When you want to visit a site anonymously, click a button and the anonymous proxy server will do the work for you.

A fuller version of the program is available on a subscription basis for $29.95 per year or $9.95 for three months. It blocks banner ads, stops pop ups, encrypts the URLs you type so that they can’t be read by your ISP or network administrator, and adds a few other features as well. I don’t find the extra features worth the money, but if these kinds of things are important to you, go ahead and spend the money. (To learn how to block pop ups, turn to “Stop Pop Ups with SP2—and Without It” [Hack #33].)

When you use this site, some sites will appear broken, with text and graphics displaying oddly. But it’s a small price to pay for your privacy.

**Use Internet Explorer for Anonymous Surfing**

If you want to surf anonymously, you don’t have to pay a service. With a bit of hackery, you can use Internet Explorer, or any other browser. To do it, you use an anonymous proxy server to sit between you and the web sites you visit.

To use an anonymous proxy server in concert with your browser, first find an anonymous proxy server. Hundreds of free, public proxy servers are available, but many frequently go offline or are very slow. To find the best one, go to http://www.atomintersoft.com/products/alive-proxy/proxy-list. The web site lists information about each server, including its uptime percentage and the last time the server was checked to see if it was online.
Surf Anonymously Without a Trace

Find the server with the highest percentage of uptime. Write down the server’s IP address and the port it uses. For example, in the listing 24.236.148.15:80, the IP address is 24.236.148.15, and the port number is 80.

In Internet Explorer, select Tools → Internet Options, click the Connections tab, and click the LAN Settings button. Check the “Use a proxy server for your LAN” box. In the Address field, type in the IP address of the proxy server. In the Port field, type in its port number. Check the “Bypass proxy server for local addresses” box, as shown in Figure 4-13; you don’t need to remain anonymous on your local network.

![Figure 4-13. Setting up Internet Explorer to surf the Web anonymously](image)

Click OK and then OK again to close the dialog boxes. Now when you surf the Web, the proxy server will protect your privacy. Keep in mind that proxy servers can make surfing the Web much slower.

Get Software for Anonymous Surfing

If you prefer to install software, get Steganos Internet Anonym 5 (http://www.steganos.com/en/sia). In addition to anonymous proxy serving, it kills pop ups and manages cookies. You can try it for free, but if you want to keep it you’ll have to pay $29.95.
See Also

• Go to http://www.gilc.org/speech/anonymous/remailer.html to send email anonymously so that it can’t be traced to you as the sender. Whistle-
blowers might want to use this feature, but others should make sure not to abuse it.
• For shareware that cleans out your cached files, destroys your history trail, and uses a variety of other methods to clean all traces of where you’ve surfed, try SurfSecret Privacy Protector (http://ww.surfsecret.com).
• “Stop Pop Ups with SP2—and Without It” [Hack #33]
• “Kill Spyware and Web Bugs” [Hack #34]
• “Take a Bite Out of Cookies” [Hack #35]
• “Don’t Get Reeled In by Phishers” [Hack #37]