How to Stay Anonymous Online

May 02, 2013 8:37 AM EST

By Neil J. Rubenking

Long-time security expert Bruce Schneier isn't the only pundit to point out that Facebook is not your product; rather, *you* are *Facebook's* product, nicely packaged for sale to its advertisers. The same can be said of any free service online. The purveyors are making money somehow, and if you're not paying, it's you they're selling.

Configuring your Facebook privacy settings keeps you from revealing your personal life outside your circle of friends, but you can't hide from Facebook itself. In general, though, there's a lot you can do to protect your privacy and anonymity online.

Help from the Browser

Modern Web browsers work hard to make your surfing experience smooth and convenient. They cache images and pages that you've viewed, so you won't have to download those items again. They keep a history of everywhere you've been, so it's easy to go back. And they retain information about your preferences in cookies, giving you personalized settings for websites. If you let them, they'll even remember your passwords.

On the other hand, anyone else who gains (or shares) access to your computer can dig into your browsing habits with ease. History and cached files reveal where you've been. Cookies restore your preferences and may automatically log you in at some sites. And a snooper who can guess your username will be able to enter secure sites using passwords saved by the browser.

You definitely don't want any browser saving your passwords. They're just not secure, as evidenced by the fact that many password manager programs can easily read and import browser-saved passwords. Dig into your browser's settings, clear any saved passwords, and turn off the option to save passwords in the future. If you need help remembering passwords (and who doesn't!) get an actual password management utility.

As for the other personal data your browser has stored, you can clear any or all of it quite easily. In Internet Explorer, Firefox, or Chrome, press Ctrl+Shift+Del to bring up a window that lets you delete whichever browsing history elements you like. You can clear data just from the last hour, if you want to conceal recent activity. Or you can clear it, as Chrome puts it, from "the beginning of time."

Stealth Browsing

Of course, a squeaky-clean browser history may suggest you have something to hide. If you're really paranoid, go ahead and *leave* traces of non-sensitive surfing in place. Then when you

want to log in to your bank or engage in an online financial transaction, switch your browser to stealth mode.

Internet Explorer's stealth mode is called InPrivate browsing. You can invoke it by right-clicking the IE icon and choosing it from the popup menu, choosing InPrivate Browsing from the Tools menu, or pressing Ctrl+Shift+P (P for private). When you right-click Firefox's icon, the stealth mode is selected by clicking "Start private browsing." You can also choose "Start Private Browsing" from the Tools menu, or press Ctrl+Shift+P.

The system works much the same way in Chrome, though the special keystroke is Ctrl+Shift+N. Choosing New Incognito Window from the menu has the same effect. In all three browsers, nothing that goes on during the private session will be retained once you close the private browsing window.

Where You At?

You can clear away all traces of browsing history, or use stealth browsing to avoid leaving any traces, but your connection with the Internet leaves its own traces. Every web page or image you see has come from a server, at the browser's request, and that server has to know your IP address in order to respond to that request.

What's the big deal? Well, from your IP address a website can get a pretty good idea of your geographical location. You can see this in action by visiting http://www.iplocation.net/ or one of the many other IP geolocation services. Websites can use this information to serve up ads targeted for your region; that's the most innocuous use.

There's a trickier use for the IP address that involves cookies and email. Vendors can send you email with a specially-formatted image link that will let them connect your email address with browsing history information they've stored in cookies. Just about every email client now blocks "remote content" to prevent this kind of snooping. The "display remote content" option subverts this protection—your best bet is to leave it alone.

Be Elsewhere

If you'd rather not broadcast your geographical location to every website you visit, consider using a Virtual Private Network, or VPN. When you use a VPN, the websites you visit never see your IP address. Instead, they see the IP address of the VPN server that's handling your traffic. For example, when I'm logged in to PCMag's own VPN, websites think I'm in New York City rather than in California.

There are plenty of free VPN utilities available, some of them quite good. Sometimes, too, there's an added bonus to faking your IP geolocation. If you want to access BBC content that's meant to be available only in England, a VPN with a London-based server will get access for you. More significantly, if you're in a country that suppresses or limits Internet access, a VPN connection to a non-restricted server may be your only chance to surf freely.

Here's one more advantage, one that protects your privacy. Everybody loves free WiFi, including the bad guys. The guy at the next table in the coffee shop may be hacking your connection, or the coffee shop's owner may be filtering all traffic, sieving out personal data. Connecting through a VPN encrypts your traffic and protects your privacy.

Stay in Balance

If analysis of your history would reveal the fact that you've been working to subvert your repressive government, well, you'd better clear that history quick. It's a matter of balance. Use a VPN when you need to cover up your geolocation, or when your connection isn't trusted. Invoke your browser's stealth mode for sensitive transactions. But if all you're doing is looking at funny cat videos, there's no real reason to hide your history (unless you're supposed to be working). Browse anonymously when it's important; hang loose when it's not.

Categories: Security

Tags: Privacy, VPN, anonymous browsing, browser

http://securitywatch.pcmag.com/security/311007-how-to-stay-anonymous-online