Pulling the shades on Internet data thieves

Michael OReilly

Starting your Web browser is like opening a window to the world — a 2-way window. As you scan the latest medical news or check out vacation spots, someone may be recording your name and your email address. They could even be poking around in your PC, determining which sites you've visited recently. They may even be storing information on your computer to keep track of you in the future.

In a recent survey of commercial Web sites — they have the suffix ".com" — the Online Privacy Alliance (www.privacyalliance.org/) determined that 92.9% of sites collected at least 1 type of personal demographic information, such as name, email address, postal address, sex and personal preferences. This is often done without the user's knowledge or consent.

I came face to face with the issue while doing research for an upcoming *CMAJ* column about online drug sales. I visited a Viagra site as part of the research, but provided it with no information. Within a half-hour the first spam email arrived, coaxing me to "BUY, BUY, BUY!!"

The Web site had automatically extracted my email address and added me to its hit list. But that's not the only thing Web sites can get from your computer without you knowing about it. To get a sense of how this works, visit the Snoop Report (www.anonymizer.com/3.0/snoop.cgi). It does the snooping and then shows you what it can find out about you.

Luckily, there are plenty of ways to pull down the shades on cyber data thieves. The best solution will depend on how you use the Internet. When it comes to email, the simplest way to ensure security is to use encryption, and some free services help users do this. One is a Web-based tool called ZipLip (www.ziplip.com/) and another is an emailer add-on that is aptly named Pretty Good Privacy (Web.mit.edu/network/pgp.html).

Both take your message and convert it into gobbledygook. The only way to make sense of it is to have the right digital key. With ZipLip this is a prearranged password, while PGP uses electronic signatures to ensure authenticity. In both cases the message remains unreadable until decoded by the recipient.

Web browsing presents greater challenges, because there are many ways an unscrupulous Web designer can get information about you, or otherwise use the 2-way connection to his own ends. Probably the most talked-about security threat has the most benign name — cookies. These small files are inserted onto your computer by a Web site and are typically used as tracers. By using cookies, a site can "remember" who you are, what services you like to use and what your local passwords are. Cookies are tremendously useful when used scrupulously. Unfortunately, not all Web sites fall into this category.

The easiest way to protect yourself against cookies is to disable them completely. In both Netscape Navigator/Communicator or Microsoft Explorer you do this within the Preferences section.

You can also determine which cookies already exist within your computer. For Explorer, go to Preferences/Receiving Files/Cookies. For Navigator/Communicator, cookie information is stored in a file called "cookies.txt". Use your computer's Find File tool to search out this item.

While you're at it, find your "history file." This contains a list of all the sites you've visited. Deleting this every few days will keep it away from unethical eyes.

If all this seems too much, take a look at the Cookie Crusher for PCS (www.thelimitsoft.com/cookie.html) or the Cookie Cutter for Mac (idirect.allmacintosh.com/files/tucows_cookiecut.hqx). Both programs will help you manage your cookies.

Aside from cookies, the biggest security problem is posed by Java and Javascript. These are small programs that run on sites to produce moving images and tally prices in e-malls. Generally, they make the Web a more interesting place to be.

Unfortunately, these little programs can also be written to access sensitive information. Some of them can read your name, email address and even get a history of where you've been visiting. Even worse, some thieves have been known to use Java to intercept private information on Web forms. This could include credit card numbers or sensitive personal information.

The solution is either to disable Java and Javascript in your Web browser's Preferences, or to use a software shield. One type of shield, a proxy server, acts as a filter and blocks prying eyes. ByProxy (www.besiex.org/ByProxy/) and the Lucent Personalized Web Assistant (lpwa.com:8000/) offer proxy servers for use on a PC.

Another option is to use the Anonymizer Web site (www.anonymizer.com/). The creators of this service let you surf through their Web site, essentially acting as your own personal proxy server. — *Michael OReilly*, moreilly@cancom.net