Preventing Privacy Invasion

Everyone has heard stories about individuals acquiring internet stalkers, identities being stolen, or personal information being tapped through computers via hackers in remote areas. Although it is easy to think that these same incidents won’t happen to you, steps and precautions should be taken to insure that your information is kept private. Plus, what can be done when companies want to know as much as possible about their customers, while consumers want to share as little as possible? Here is some brief background information about internet privacy rights as well as a few tips for protection.

The right to privacy is not derived from any single source, however the Declaration of Human Rights states that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks upon his honor or reputation.” The right to privacy is also protected by the Privacy Act of 1974 and found implicitly through the first, third, fourth and fifth amendments of the United States Constitution. Individual digital privacy, however, has been met with congressional indecisiveness, due to the conflicted goal of stemming or aiding internet advancement, yet some acts have been passed to protect individual’s rights via electronic modes. The Electronic Communications Privacy Act (ECPA) and the Communications Decency Act (CDA) in which Congress stated that “the United States [should] promote the continued development of the Internet and other interactive computer services and other interactive media.”

In most US states, employees have little if any privacy protection from monitoring by employers. Follow the rule, if it’s private, do it at home. See this article on “snoopware” (which may not be limited to your office...)

With so little legislation on what companies must do to keep their internet user’s information private, gathering information without notice becomes an issue. As customers search websites, nearly every click is tracked, documenting what individuals search. As a story in the Washington Post revealed, 11 pharmaceutical companies - including Pfizer Inc., SmithKline Beecham PLC, Glaxo Wellcome PLC - had formed an alliance and were tracking every click consumers made across their sites, then comparing notes to better tailor their advertisements. Consumers were never told. (MSNBC.) The same tracking is undoubtedly happening to you. Look at the advertisement banners that appear on the websites that you search. Do the products look familiar? Perhaps you search for them regularly.

So, in a world where every click is traced and information can be shared and traded so easily, what can be done to maintain privacy? The Electronic Frontier Foundation offers 9 tips to help protect your privacy.

1) Do not reveal personal information inadvertently.
   As you navigate through sites you may be sharing personal details, including e-mail addresses and other contact information, without even knowing it. To prevent this, make sure you properly configure your Web browser. In your browser's "Setup", "Options" or "Preferences" menus, you are able to opt to use a pseudonym. When visiting a site you trust you can choose to give them your info via the site's own forms, but your information does not need to be public to everyone as you navigate the web. Also be on the lookout for system-wide "Internet defaults" programs on your computer (some examples include Window's Internet Control Panel, and MacOS's Configuration Manager, and the third-party Mac utility named Internet Config). While they are useful in a variety of ways, like keeping multiple Web browsers and other Internet tools consistent in how the treat downloaded files, they should probably also be anonymized just like your browser itself.

2) Turn on cookie notices in your Web browser
   "Cookies" are tidbits of information that Web sites store on your computer to obtain information about your internet search activities. For a demonstration of how they work, see: http://privacy.net/track/

   Browsers are starting to allow user control over cookies or you can also use cookie management software and services. Some examples are Internet Junkbuster Proxy (http://www.junkbusters.com/Ihti/engl.html), interMute (http://www.intermute.com/), GuideScope (http://www.guidescope.com/home/), Muffin (http://muffin.doit.org/), Web Washer (http://www.webwasher.com/), CookiePal (http://www.kburra.com/cpal.html), and The Limit Soft (http://www.thelimitsoft.com/cookie.html). There are also numerous "cookie eater" applications, some which run on a schedule or in the background, that delete cookie files for you.

3) Keep a "clean" e-mail address.
   Everyone has signed up for a service, website, or group that has required an e-mail address. Create an account for this purpose only to keep your real account free from spam e-mail. Also, if you must check the account for a code that is sent to you, you can use "someone@example.com" (example.com is a non-existent site, set up by the Internet standards to be used as an example that will never accidentally coincide with anyone's real e-mail address, which is always a danger if you just make up one off the top of your head.)

4) Don't reveal personal details to strangers or "friends".
   Due to the issue with never seeing someone's true identity, it is very easy for internet users to lie about their identity on internet chat rooms or networking sites. Even if the person that you are in correspondence with may seem trustworthy, a 14-year-old girl can really be a 40-year-old man. Never share your full name, school, places where you live, work, or hang out, credit card information, social security number or any specific identifying information online. If meeting an online contact in person, make sure that you meet in a public place during the daytime and always involve other people.

5) Realize you may be monitored at work.
   In most US states, employees have little if any privacy protection from monitoring by employers. Follow the rule, if it's private, do it at home. See this CNN article on "snoopware" which may not be limited to your office...
6) Beware sites that offer a reward or prize in exchange for your contact information and personal details.

If a prize is awarded for sharing your information, then the company is most likely collecting data solely for marketing purposes, and in many cases selling it to other, sometimes not so reputable companies.

7) Do not reply to spammers, for any reason.

Replying to a "spam" e-mails is not a good way to block them from your lists. Try using these programs to stop spam e-mails:

- Spam Hater (http://www.cix.co.uk/~net-services/spam/spam_hater.htm) for Windows users;
- TAG (http://alcor.concordia.ca/topics/email/auto/procmail/spam) for experienced Unix users;
- SpamBouncer (http://www.spambouncer.org) for experienced Unix users (works well with TAG);
- BrightMail (http://www.brightmail.com/) for ISPs;
- SpamCop (http://spamcop.net/) for anyone;
- More information on fighting spam is available at:
  - Elsop's Anti-Spam Page (http://www.elsop.com/wrc/nospam.htm);
  - MaximumDownforce's Info-n-Links Page (http://www.maximumdownforce.com/hotlinks.html);
  - Whew's Anti-Spam Campaign (http://www.whew.com/Spammers/).

Many of these are difficult to use for novices, and some require Unix expertise. Others are services that deal with ISPs only, not end users.

8) Remember that YOU decide what information about yourself to reveal, when, why, and to whom.

Think twice about giving out phone numbers, zip codes, and e-mail addresses, even when you aren't online. If a sales clerk asks for an e-mail address to enter into a computer system while shopping, your information can still be stolen. Be careful when making up e-mail addresses and addresses as well, be courteous enough to make something obviously fake so as not to spam someone else's account.

9) Use encryption!

If using a wireless internet source, make sure that your network is hidden and the password is encrypted so as not to allow hackers easy access to your network.