EFF's Top 12 Ways to Protect Your Online Privacy

by Stanton McCandlish, EFF Technology Director, *Apr. 10, 2002*

1) Do not reveal personal information inadvertently.

You may be "shedding" personal details, including e-mail addresses and other contact information, without even knowing it unless you properly configure your Web browser. In your browser's "Setup", "Options" or "Preferences" menus, you may wish to use a pseudonym instead of your real name, and not enter an e-mail address, nor provide other personally identifiable information that you don't wish to share. When visiting a site you trust you can choose to give them your info, in forms on their site; there is no need for your browser to potentially make this information available to all comers. 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 for various things, like keeping multiple Web browers and other Internet tools consistent in how the treat downloaded files and such, they should probably also be anonymized just like your browser itself, if they contain any fields for personal information. Households with children may have an additional "security problem" - have you set clear rules for your kids, so that they know not to reveal personal information unless you OK it on a site-by-site basis?

2) Turn on cookie notices in your Web browser, and/or use cookie management software or infomediaries.

"Cookies" are tidbits of information that Web sites store on your computer, temporarily or more-or-less permanently. In many cases cookies are useful and inocuous. They may be passwords and user IDs, so that you do not have to keep retyping them every time you load a new page at the site that issued the cookie. Other cookies however, can be used for "data mining" purposes, to track your motions through a Web site, the time you spend there, what links you click on and other details that the company wants to record, usually for marketing purposes. Most cookies can only be read by the party that created them. However, some companies that manage online banner advertising are, in essence, cookie sharing rings. They can track which pages you load, which ads you click on, etc., and share this information with all of their client Web sites (who may number in the hundreds, even thousands.) Some examples of these cookie sharing rings are DoubleClick, AdCast and LinkExchange. For a demonstration of how they work, see: http://privacy.net/track/

Browsers are starting to allow user control over cookies. Netscape, for example, allows you to see a notice when a site tries to write a cookie file to your hard drive, and gives you some information about it, allowing you to decide whether or not to accept it. (Be on the lookout for cookies the function of which is not apparent, which go to other sites than the one you are trying to load, or which are not temporary). It also allows you to automatically block all cookies that are being sent to third parties (or to block all cookies, entirely, but this will make some sites inoperable). Internet Explorer has a cookie management interface in addition to Netscape-like features, allowing you to selectively enable or disable cookies on a site-by-site basis, even to allow cookies for a site generally, but delete a specific cookie you are suspicious about. With Internet Explorer you can also turn on cookies for a site temporarily then disable them when you no longer need them (e.g., at an online bookstore that requires cookies to process an order, but whom you don't want to track what books you are looking at, what links you are following, etc., the rest of the time.) Turning on cookie warnings will cause alert boxes to pop up, but after some practice you may learn to hit "Decline" so fast that you hardly notice them any more. The idea is to only enable cookies on sites that require them AND whom you trust. You may also wish to try out "alternative" browsers like Mozilla (Windows, Mac, Linux), Opera (Windows, Mac, Linux), Konqueror (Linux), and iCab (Mac), which may offer better cookie management.

You can also use cookie management software and services. One example is the Internet Junkbuster Proxy (http://www.junkbusters.com/ht/en/ijb.html). It runs on Win95/98/NT and Unix/Linux (no Mac version), and can selectively block cookies for you (and banner ads, to boot). interMute (http://www.intermute.com/) does likewise (and more - blocks popup windows, etc.; only runs under Windows). Another Windows-only solution is AdSubtract (http://www.adsubtract.com/) A comparable product (Linux, Solaris, Windows) is GuideScope (http://www.guidescope.com/home/) A Java-based solution called Muffin (http://muffin.doit.org/) is also available. While it will run on Mac, Windows and Unix systems, it is definitely for "power users", as it is complicated to set up and operate effectively. Another recent option (Linux, Mac, Windows) is the (http://www.webwasher.com/), which has advanced cookie filtering capabilities, especially with the Seclude-It and Secretmaker plug-ins available at the same site. One more (Windows) is CookiePal (http://www.kburra.com/cpal.html), and yet another (Windows) is (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. As with turning off cookies entirely, you may have trouble accessing sites that require certain cookies (though in most cases the worst that will happen is that you'll have to re-enter a login ID and password you thought were saved.) "Eating" the cookies periodically still permits sites to track what you're doing for a short time (i.e., the time between successive deletion of your cookie file), but thwarts attempts to discern and record your actions over time.

Yet another option is to use an "infomediary" (some are home-use software products, others may be network-based services), such as SeigeSoft's SiegeSurfer (http://www.siegesoft.com/_html/tutorial.asp), Zero Knowledge Systems' Freedom (http://www.freedom.net), among others. These products/services act as a proxy or shield between you and sites you visit, and can completely disguise to Web sites where you are coming from and who you are (and intercept all cookies). Most are Windows-only at this point, though Anonymizer (http://www.anonymizer.com/3.0/affiliate/door.cgi?CMid=13763), Orangatango

(http://www.orangatango.com/), and SafeWeb and (http://www.safeweb.com) also offer such services that are Web-based and not platform-dependent. WARNING: Do not confuse honest infomediaries with "identity managmenet services" like Microsoft's Passport service or Novell's DigitalMe. While you may gain some temporary convenience at sites that support them, you'll lose essential privacy, because these services are not there to serve you but to serve marketing purposes by collecting a vast array of information about you and selling it.

The best solution doesn't exist yet: Full cookie management abilities built into the browsers themselves. Only increased user pressure on Microsoft, Netscape and other browser makers can make this happen. Users should ultimately be able to reject cookies on a whole-domain basis, reject all third-party cookies by default, reject all cookies that are not essential for the transaction at hand, receive notice of exactly what a cookie is intended for, and be able to set default behaviors and permissions rather than have to interact with cookies on a page-by-page basis. This just isn't possible yet. You may wish to contact the company that makes your browser software and demand these essential features in the next version.

3) Keep a "clean" e-mail address.

When mailing to unknown parties; posting to newsgroups, mailing lists, chat rooms and other public spaces on the Net; or publishing a Web page that mentions your e-mail address, it is best to do this from a "side" account, some pseudonymous or simply alternate address, and to use your main or preferred address only on small, members-only lists and with known, trusted individuals. Addresses that are posted (even as part of message headers) in public spaces can be easily discovered by spammers (online junk mailers) and added to their list of targets. If your public "throw away" address gets spammed enough to become annoying, you can simply kill it off, and start a new one. Your friends, boss, etc., will still know your "real" address. You can use a free (advertising-supported) e-mail service provider like Yahoo Mail or Hotmail for such "side" accounts. It is best to use a "real" Internet service provider for your main account, and to examine their privacy policies and terms of service, as some "freemail" services may have poor privacy track records. You may find it works best to use an e-mail package that allows mulitiple user IDs and addresses (a.k.a. "personalities", "aliases") so that you do not have to switch between multiple programs to manange and use more than one e-mail address (though you may have to use a Web browser rather than an e-mail program to read your mail in your "throw away" accounts - many freemail providers do not allow POP or IMAP connections). If you are "required" to give an e-mail address to use a site (but will not be required to check your mail for some kind of access code they send you), you can use "someuser@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 just-met "friends".

The speed of Internet communication is often mirrored in rapid online acquaintanceships and friendships. But it is important to realize that you don't really know who these people are or what they are like in real life. A thousand miles away, you don't have friends-of-friends or other references about this person. Be also wary of face-to-face meetings. If you and your new e-friend

wish to meet in person, do it in a public place. Bringing a friend along can also be a good idea. One needn't be paranoid, but one should not be an easy mark, either. Some personal information you might wish to withhold until you know someone much better would include your full name, place of employment, phone number, and street address (among more obvious things like credit card numbers, etc.) Needless to say, such information should not be put on personal home pages. (If you have a work home page, it may well have work contact information on it, but you needn't reveal this page to everyone you meet in a chat room.) For this and other reasons, many people maintain two personal home pages, a work-related one, and an "off duty" version. In the commercial sector, too, beware "fast-met friends". A common "social engineering" form of industrial espionage is to befriend someone online just long enough to get them to reveal insider information.

5) Realize you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer.

In most US states and many if not most countries, employees have little if any privacy protection from monitoring by employers. When discussing sensitive matters in e-mail or other online media, be certain with whom you are communicating. If you replied to a mailing list post, check the headers - is your reply going to the person you think it is, or to the whole list? Also be aware that an increasing number of employers are monitoring and recording employee Web usage, as well as e-mail. This could compromise home banking passwords and other sensitive information. Keep private data and private Net usage *private*, at home. See this *CNN*/*IDG* article on "snoopware" (which may not be limited to your office...):
http://www.cnn.com/2001/TECH/ptech/11/07/snoopware.idg/

6) Beware sites that offer some sort of reward or prize in exchange for your contact information or other personal details.

There's a very high probability that they are gathering this information for direct marketing purposes. In many cases your name and address are worth much more to them because they can sell it to other marketers (who can do the same in turn...) than what you are (supposedly) getting from them. Be especially wary of sweepstakes and contests. You probably won't win, but the marketer sure will if you give them your information.

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

"Spam", or unsolicited bulk e-mail, is something you are probably already familiar with (and tired of). If you get a spammed advertisment, certainly don't take the sender up on whatever offer they are making, but also don't bother replying with "REMOVE" in the subject line, or whatever (probably bogus) unsubscribe instructions you've been given). This simply confirms that your address is being read by a real person, and you'll find yourself on dozens more spammers' lists in no time. If you open the message, watch your outgoing mail queue to make sure that a "return receipt" message was not generated to be sent back to the spammer automatically. (It is best to queue your mail and send manually, rather than send immediately, so that you can see what's about to go out before it's actually sent. You should also turn off your mailer's automatic honoring of return receipt requests, if any.) If you have a good Internet service provider, you

may be able to forward copies of spam e-mail to the system administrators who can route a complaint to the ISP of the spammer (or if you know a lot about mail headers and DNS tools, you can probably contact these ISPs yourself to complain about the spammer.) If you are getting spammed a lot, there are a variety of filters and anti-spam services available, including:
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) Be conscious of Web security.

Never submit a credit card number or other highly sensitive personal information without first making sure your connection is secure (encrypted). In Netscape, look for an closed lock (Windows) or unbroken key (Mac) icon at the bottom of the browser window. In Internet Explorer, look for a closed lock icon at the bottom (Windows) or near the top (Mac) of the browser window. In any browser, look at the URL (Web address) line - a secure connection will begin "https://" intead of "http://". If you are at page that asks for such information but shows "http://" try adding the "s" yourself and hitting enter to reload the page (for Netscape or IE; in another browser, use whatever method is required by your browser to reload the page at the new URL). If you get an error message that the page or site does not exist, this probably means that the company is so clueless - and careless with your information and your money - that they don't even have Web security. Take your business elsewhere.

Your browser itself gives away information about you, if your IP address can be tied to your identity (this is most commonly true of DSL and broadband users, rather than modem users, who are a dwindling minority). For a demo of how much detail is automatically given out about your system by your browser, see: http://privacy.net/analyze/ .

Also be on the lookout for "spyware" - software that may be included with applications you install (games, utilities, whatever), the purpose of which is to silently spy on your online habits and other details and report it back to the company whose product you are using. One MS Windows solution for disabling spyware is the Ad-aware program (shareware, from http://www.lavasoft.de/), which can remove spyware from your computer; it is based on a large collaboratively maintained database of information about spyware. Linux and Mac products of this sort are likely to appear soon.

Java, Javascript and ActiveX can also be used for spyware purposes. Support for these scripting languages can be disabled in your browser's configuration options (a.k.a. preferences, settings, or

properties). It is safest to surf with them turned off, and only turn them on when a site you trust and want to use requires them. If you don't know if your browser supports these languages or don't know if they are turned on you can use BrowserSpy to find out (along with a lot of other information about your Web browsing software): http://gemal.dk/browserspy/

Another form of spyware consists of "webbugs", which typically manifest themselves as invisible or nearly invisible image files tied to cookies and javascripts that track your Web usage. See http://www.google.com/search?hl=en&q=webbugs+%22web+bugs%22 for more information on webbugs. See also this webbug FAQ, http://www.nthelp.com/OEtest/web_bug_faq.htm for more details. Dealing with webbugs when they are embedded in an otherwise legitimate page is thorny, as there isn't a surefire way to distinguish between webbugs and run-of-the-mill image files. But see the Privacy Foundation's Bugnosis webbug detector (http://www.bugnosis.org/ - Windows MSIE only). When webbugs are loaded into popup pages, the solution is to close the popups (usually a small page with an ad, though some of them are "micropages" that you can barely see. A few may even use javascript tricks to keep you from closing them. If this happens, close all other browser windows, then you should be able to close the bug window). Another tip for defeating webbugs is to reject any cookies from Doubleclick, AdCast, LinkExchange and other "ad exchange networks" (cookie sharing rings), and any other cookies that are not from the site you are currently visiting (most third-party cookies are basically webbugs). Lastly on this topic, be aware that HTML-capable e-mail programs and Usenet newsreaders make webbugs work in your e-mail and newsgroups. If your mailer or newsreader has an option to turn off cookie support, you should certainly do so. There is hardly any imaginable legitimate use for a cookie in an email or a newsgroup posting.

9) Be conscious of home computer security.

On the other side of the coin, your own computer may be a trouble spot for Internet security. If you have a DSL line, broadband cable modem or other connection to the Internet that is up and running 24 hours (including T1 at the office without a firewall or NAT), unlike a modem-and-phone-line connection, be sure to turn your computer off when you are not using it. Most home PCs have pitifully poor security compared to the Unix workstations that power most commercial Web sites. System crackers search for vulnerable, unattended DSL-connected home computers, and can invade them with surprising ease, rifiling through files looking for credit card numbers or other sensitive data, or even "taking over" the computer and quietly using it for their own purposes, such as lauching attacks on other computers elsewhere - attacks you could initially be blamed for. Firewall hardware and software is another option that can protect you from these kinds of attacks (available at any computer store; freeware and shareware implementations may be available at sites like http://www.shareware.com or http://www.download.com.

10) Examine privacy policies and seals.

When you are considering whether or not to do business with a Web site, there are other factors than a secure connection you have to consider that are equally important to Web security. Does the site provide offline contact information, including a postal address? Does the site have a prominently-posted privacy policy? If so, what does it say? (Just because they call it a "privacy policy" doesn't mean it will protect you - read it for yourself. Many are little more than

disclaimers saying that you have no privacy! So read them carefully.) If the policy sounds OK to you, do you have a reason to believe it? Have you ever heard of this company? What is their reputation? And are they backing up their privacy statement with a seal program such as TRUSTe (http://www.truste.org/) or BBBonline (http://www.bbbonline.org/)? (While imperfect, such programs hold Web sites to at least some minimal baseline standards, and may revoke, with much fanfare, the approval-seal licenses of bad-acting companies that do not keep their word.) If you see a seal, is it real? Check with the seal-issuing site to make sure the seal isn't a fake. And examine terms carefully, especially if you are subscribing to a service rather than buying a product. Look out for auto-rebilling scams and hidden fees.

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

Don't give out personally-identifiable information too easily. Just as you might think twice about giving some clerk at the mall your home address and phone number, keep in mind that simply because a site asks for or demands personal information from you does not mean you have to give it. You do have to give accurate billing information if you are buying something, of course, but if you are registering with a free site that is a little too nosy for you, there is no law (in most places) against providing them with pseudonymous information. (However, it would probably be polite to use obviously fake addresses, such as "123 No Such Street, Nowhere, DC 01010". If they are generating mailings based on this information - presumably in accordance with the terms of their privacy policy - they can probably weed such addresses out and not waste the postage on them. Definitely do NOT use someone else's real address!) However, if you are required to agree to terms of service before using the free service, be sure those terms do not include a requirement that you provide correct information, unless the penalty is simply not being allowed to use the service any more, and you're willing to pay that price if they figure out you are not providing them with your actual personally-identifiable information.

12) Use encryption!

Last but certainly not least, there are other privacy threats besides abusive marketers, nosy bosses, spammers and scammers. Some of the threats include industrial espionage, government surveillance, identity theft, disgruntled former associates, and system crackers. Relatively easy-to-use e-mail and file encryption software is available for free, such as Pretty Good Privacy (PGP, available at: http://www.pgpi.org/), which runs on almost all computers and even integrates seamlessly with most major e-mail software. Good encryption uses very robust secret codes, that are difficult if not impossible to crack, to protect your data. You can also use specialized services (some free, some pay) that go beyond infomediary services, including running all connections through a securely encrypted "tunnel", anonymous dialup, even anonymous Web publishing. Anonymizer (http://www.anonymizer.com/3.0/affiliate/door.cgi?CMid=13763) offers all of these services. Another type of product is SSH tunnelling (port forwarding) packages, such as FSecure SSH (http://www.fsecure.com/products/ssh/), and SecureCRT (http://www.vandyke.com/products/securecrt/).

Hopefully some day soon, good encryption and computer security will simply be included in all ISP services and operating systems, but for now you have to actively seek out good service providers and add-on products.

For more information on protecting your online privacy:

- EFF Privacy Archive - http://www.eff.org/Privacy/
- "Protecting Yourself Online" Book - http://www.eff.org/promo/books.html#protect
- TRUSTe's "Protecting Your Privacy Online" FAQ - http://truste.org/consumers/users_faqs.html
- Privacy Rights Clearinghouse - http://www.privacyrights.org/
- Privacy International - http://www.privacyinternational.org/

Note: Mention of specific product, service or company names does not constitute EFF endorsement or recommendation. Examples and links are provided as starting points for readers, who must make up their own minds about how much security they need and whether particular offerings will suit their needs.

For information about the law and technology of government surveillance in the United States, check out EFF's Surveillance Self-Defense project.

http://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy