Wanted: Cookies, Web Bugs and Viruses - How to Protect your Privacy on the Internet

Wanted: Cookies, Web Bugs and Viruses - How to Protect your Privacy on the Internet

Insight — 6/18/2001 12:00:00 AM

Are you concerned about your on-line privacy on the Internet? Studies have shown that more than 50% of Internet users are willing to share personal information in order to use a Web site and that they don't worry about the Web sites they have visited. Here are some suggestions to help protect your privacy:

- On-line purchases - designate one (1) credit card to make purchases via e-commerce. It is easier to cancel one (1) credit card if it is stolen versus several credit cards. In addition, if your purchases are tax deductible, it is easier to use only one card to reconcile purchases for the IRS.

- Make sure on-line stores have secure servers - generally the site usually identifies itself as a secure site.

- Create a unique password - don't use birthdates, names of pets or your social security number. Add a number in the middle of the alpha character password.

- Don't maintain a browser cache. To clean out your cache in Internet Explorer 5, simply click on TOOLS / INTERNET OPTIONS / GENERAL TAB / DELETE FILES IN TEMPORARY INTERNET SECTION. To clean out your cache in Netscape 4, click on EDIT / PREFERENCES / ADVANCED / CACHE / CLEAR MEMORY CACHE / CLEAR DISK CACHE.

- Don't share or rent your address or name. Consider masking your ID through using an anonymizing service available on the Internet. Many sites will hide your actual IP address and substitute their own.

- Remove your name from mailing lists - this will reduce the

possibility of being spammed. Also don't respond to unsolicited junk mail!

- Be aware of Web sites that offer rewards or prizes in exchange for your name, address and other personal information. The more personal information you provide, the less privacy you have as an individual.

- Encryption - Extra security regarding e-mails - no one else but you and the intended recipient can decipher the message. There are several Web based programs you can access to determine which best fits your needs.

- Cookies are an HTTP header that includes a text-only string (domain, path, lifetime and value of variable that a Web site sets) that gets entered into the memory of the browser. Both Netscape and Microsoft Internet Explorer limit the number of cookies that will be saved on your hard drive at one time. A cookie alone cannot read your hard drive to find out who you are and where you live. The only way this information could end up as a cookie is if YOU provide the information to the site and then the site saves it to a cookie. So, why do sites use cookies?

Simple, they want to personalize their services to you, i.e. Amazon Books will remember you like to read non-fiction books and airlines will remember you like to travel in Europe on an annual basis. Did you know that agencies within our own Federal Government are using cookies to track habits of users despite rules prohibiting the practice? Tracking Internet users' preferences is an effective marketing tool for e-commerce. Can you delete cookies? Yes, but remember to close your browser first because cookies are held in memory until your browser is closed. Both Netscape and Microsoft Internet Explorer allow you to screen your incoming cookies and delete those cookies that are suspicious. Check out www.guidescope.com for further information for setting cookie rules for each site you visit.

"Web bugs" are small GIF images (invisible graphic files) embedded in Web pages that report back to the company information they are seeking to obtain. To avoid Web bugs you can disable image loading into your browser however this may be a tough trade-off for your other graphic software applications.

- Don't share or provide personal information to questionnaires, i.e. social security number, medical history, financial information (bank account number, credit history, savings, mortgage account information), employment history or e-mail address.

- A firewall watches traffic coming into your PC and acts as a gatekeeper for potential hackers. High speed connections using a broadband connection such as DSL or cable should have a software firewall. PC World recommends BlackICE Defender 2.1 or ZoneAlarm Pro.

- Store sensitive information on a removal drive, i.e. trademark, patent infringement, confidential documents or transactional related documents.

- Beware of shared ware received as an attachment to an e-mail or a download from the Internet. Don't open unfamiliar attachments that may be infected with a virus (how often do we receive e-mails from our friends warning us of the latest virus attacking computer networks?).

- Turn off your computer when not in use to minimize break in time. A situation may arise when you have un-invited guests or visitors in your office who may be computer savvy and access proprietary information maintained by your company or law firm.

Want more information regarding privacy - check out these Web sites:

www.junkbusters.com - articles related to privacy issues and profiling users

www.anonymizer.com - blocks all cookies and disguises where you are coming from and who you are

www.ftc.gov/privacy/ - Federal Trade Commission - information regarding congressional testimony, legislative hearings' updates

---