

Tip of the month

Getting Stuffed With Cookies When You Browse?

Based upon the article by Rich Luhr. Published in Internet Medicine, March, 1997

Although it's easy to get the impression when browsing the web that one is doing so anonymously, your activities might be tracked in several ways. One of the most popular techniques for tracking usage is the "cookie", and even if you've heard of them before, you might be surprised at what they can do.

A cookie is like a passport in your computer. Whenever you visit a web site, the web server can send a cookie to your computer, which is then stored on your hard drive. As you visit additional sites, you may pick up additional cookies. Each cookie can be a miniature record of your visit to a specific web site, complete with information such as an ID number, time of your last visit to that specific site, and any other information that you give up willingly such as password or email address.

The effect is something akin to "Caller ID" on telephones. By retrieving the cookie left previously, a web site can "remember" your site-specific password, your preferences, and other tidbits of information. When you re-visit a site, a cookie left on your hard drive will identify you.

In other cases, cookies are being used to keep track of how many visitors visit a site. These types of cookies don't get stored permanently in your computer they expire immediately, so they can't be used to determine how often you re-visit the site. Advocates of cookies point out that cookies can streamline and improve your use of web sites. For example, when visiting The New York Times Online (www.nytimes.com), you will only have to enter your password once. The next time you visit, a cookie will tell the web server who you are and you'll be able to bypass the usual password-protected sign-on screen.

On the other hand, The New York Times could easily track how often you visit their site, what sections of the paper you read, and even estimate how long you spent there. Naturally, discovering the existence of such a tracking mechanism has created some alarm among web users. Although cookies aren't intrinsically malevolent, many have foreseen that cookies could be used to develop a profile of individuals which could then be used for marketing, or perhaps more nefarious, purposes. Privacy advocates consider this to be potentially an invasive act.

We'll tell you how to disable cookies in your web browser later in this article, but first, some Q&A about cookies will help you understand what they can and cannot do.

Q: When is a cookie really useful to me?

A: One of the most popular applications of cookies is the "shopping cart". Sites like L.L. Bean use cookies to keep track of your purchases while you shop in their virtual store. This can be accomplished without cookies, as well so even if you disable cookies you may be able to utilize such sites. For now, most web sites are using cookies just to

Tip of the month

accomplish what other sites achieve using passwords and registration forms. Cookies generally only streamline the process.

Q: What can't cookies do?

A: Cookies cannot enable the web server to read from your hard drive, get your e-mail address against your will, destroy files on your computer, or create executable programs. Cookies can only contain as much information about you as you disclose on the site that sets the cookie.

Q: If a cookie is stored on my hard drive, won't that consume a lot of disk space eventually?

A: Not really. Cookies are limited to 4k in size, and most are much smaller, so you would have to visit thousands of web sites using cookies to consume even a single megabyte of disk space.

Q: Who can see my cookies?

A: A cookie is specific to a web server. Only the web server that set the cookie initially can retrieve it later. So, no one can retrieve all of your cookies to develop a profile of your web browsing habits.

Q: Since they're downloading something to my hard drive, should I be concerned about viruses?

A: No, cookies are limited to text-only, and can't be executed. Therefore, it's impossible that a cookie could contain a virus.

Q: Can web sites use cookies to see where I've been previously?

A: No, but surprisingly, any web site can get information regarding what operating system and browser software you are using (for example, Win/Netscape), and the address of the last site you visited without using cookies!

Q: Do they ever go away?

A: All cookies have expiration dates (like the store-bought kind), but usually those expiration dates are either years in the future, or immediately after the web session ends, depending on what the cookie is being used for.

Q: Are cookies a security risk?

A: They could be, in a small way. If your computer is networked to others, there is a possibility that someone could access your cookie file and read it. If some of your cookies contained passwords that you use for particular web sites, that information would be readily available. To combat this, most web sites don't set cookies with anything more than an encrypted ID number. You should also make a habit of using different passwords for web sites than you do for more critical things, like locking your computer or your ATM card.

If you want to get examine what cookies you've already accumulated, look for a file called COOKIES.TXT on your hard drive (usually located on the D drive under Documents and Settings.)

Killing The Cookie Monster

If you've decided you don't want to be tracked with cookies, you have several options: First, you can tell Microsoft Explorer to alert you whenever a web site is trying to set a cookie on your computer. Go to the Control Panel (from My Computer), and click on the

Tip of the month

Internet Options icon, select Privacy, then select the Advanced tab. Check Override automatic cookie handling and click on Prompt for both first party cookies and third party cookies. Click Apply and or Ok to save the settings.

If you follow this procedure, you'll get a warning every time a cookie is sent and be able to choose whether to allow it or not. If you select "Cancel", the cookie won't be set. In most cases, the web site acts normally, but in some cases this can cause the web site to display incorrectly. The disadvantage of this method is that some sites attempt to send a cookie with every image; meaning that you can be clicking "Cancel" a lot before the web site finally appears.

Neither Internet Explorer nor Navigator allow you to turn off cookies completely, so your second option to kill the cookie monster is a little more extreme: You can periodically locate and delete the contents of the file COOKIES.TXT. This will, of course, wipe out all cookies stored on your computer. Theoretically, you could also edit out only the cookies you don't want, using a text editor. Think of this as "tossing your cookies".

Overall, cookies are like most other bits of technology: useful if used properly, but dangerous if mismanaged. If you dislike others tracking your use of their website, then you have options to protect yourself. If you are ambivalent about being tracked, then cookies can be very useful, and best of all, they are completely automatic.