From: Steve Gimnicher <steve@gimnicher.com>
Subject: Communication from your Computer Guy: Browser Cookies
Date: April 15, 2012 10:38:48 AM PDT

1 Attachment, 10 KB

I suspect that most of you have heard of browser cookies in the context of something to worry about when you are browsing the Internet, but aren't really sure what they can and cannot do. In this month's newsletter, all will be explained.

According to Wikipedia, the term "cookie" was derived from "magic cookie" and was invented in 1994 by a Netscape founding engineer named Lou Montulli.   Cookies are an Internet browsing mechanism used by a website to send information to a user's browser where it is stored, and for the browser to return the same information to the same site the next time it is visited. Simply put, cookies are a mechanism for websites to remember information between visits. This information can be anything related to the user's interaction with the web site, including authentication data, session data, user preferences, and shopping cart contents. Fundamentally, cookies cannot be programmed and therefore cannot execute code on your computer, so they are incapable of installing viruses or other malware. However, since they do contain private information, they are a target for a variety of malicious techniques (too technical to be explained in this article. If you are interested, I refer you to the "Cookie theft and session hijacking" section at http://en.wikipedia.org/wiki/HTTP_cookie).

Cookies also serve a major role as a mechanism for advertisers to gather information about your browsing habits so that they can serve targeted ads to you during your browsing session. Let's walk through an example to see how this works. Let's say that you visit www.mysite.com. On that site, you might see ads that have been placed there by www.great-ads.com. Later, when you visit another site, such as www.another-site.com, you might also see ads that have been placed there by www.great-ads.com. This ad placement occurs via the instructions (HTML) sent by the web server that hosts the requested web pages to your web browser. The instructions tell the browser exactly where to place the ad and to go get the ad from www.great-ads.com.

This is where cookies come in. Whenever your browser gets information from a web site, the web site has the opportunity to store cookies on your computer. So, www.mysite.com can store cookies, but when www.great-ads.com is referenced, it too can store cookies on your computer. The cookies stored by www.great-ads.com are called "third party cookies" (you are the first party, www.mysite.com is the second party, and www.great-ads.com are the third party).

Third parties can use their cookies for tracking purposes (called "tracking cookies"). This works as follows: when you visit www.mysite.com and it calls www.great-ads.com for the first time, www.great-ads.com places a cookie on your computer that says "this is visitor 25,273,128". You then go to www.another-site.com, who also calls www.great-ads.com. Since www.great-ads.com already has a cookie stored on your computer, it is sent to www.great-ads.com. www.great-ads.com sees the cookie it stored earlier that says "this is visitor 25,273,128". So, www.great-ads.com now knows that you visited both www.mysite.com and www.another-site.com. Since www.great-ads.com is a major Internet web site, it can analyze a significant amount of information to determine browsing habits and target ads. In much the same way, search engines can also track your searching habits and learn a lot about you.

There have been many advances to help protect your privacy. Most current versions of web browsers have an "in private" browsing option, where pages you have viewed aren't stored in your browsing history and cookies are automatically deleted when you close all open windows. There are also a variety of browser settings that limit or eliminate use of cookies. Many software vendors also offer products to protect your privacy. Major web sites (e.g., Facebook, Google, etc) offer their users a wide variety of privacy settings that they can control.

I encourage you to research these options, but you have to be practical as well. Most major web sites will not work properly with cookies disabled, and cookies are certainly very convenient when revisiting your favorite web sites. It is extremely unlikely that anyone is tracking you personally; these mechanisms exist to improve your on line experience by making it more relevant and easy for you. As long as you are vigilant, visit legitimate web sites, use common sense, and keep all your software and especially antivirus updated, you should be safe.

As always, I hope you have found this information useful. If you do not wish to receive these emails in the future, let me know. This newsletter, as well as all past newsletters, can be found on my web site (www.gimnicher.com/steve).

Steve Gimnicher
Gimnicher Computer Services
www.gimnicher.com/steve
650-222-4140
steve@gimnicher.com