No. 134, February 2007

THE COMPUTER CORNER

No. 134. Cookies Revisited

- by Stan Kaplan, WB9RQR
715 N. Dries Street
Saukville, WI 53080-1664
(262) 268-1949
skaplan@mcw.edu

I wrote about cookies over seven years ago (#68, Cookies, Jul 99), and it is time to revisit the subject. In that article I mentioned that cookies are small text-only files, downloaded to your hard drive by a web site you visit (or even a web site you do not visit), and that they may persist there, taking space like any other file, for hours, days, weeks, months or years. Why might they persist? Even though the expiration date for a cookie has passed (they all have such a date), no one comes back to erase them. The purveyors of web pages that you visit are not interested in cleaning house on your machine. Just adding cookies.

Cookies are actually a form of spyware. They are generally placed on your hard drive without your knowledge and informed consent. And they return information to the site that put them on your hard drive without your knowledge and informed consent.

Cookies do have some positive value for you. They can store your preferences, so that when you log on to PartsForLess.com, their server can read the cookie it placed on your machine when you last visited their site, and it therefore knows you are interested in DVD-ROM drives, so it takes you right to that section on its site. When you log onto LatestNews.com, their server reads the cookie it set last time you visited, and it knows you are interested in sports rather than international news, so it takes you to the latest football scores. Without cookies, each time you visit a site would be a first-time occurrence, as far as that website is concerned. So, cookies can personalize your surfing experience.

On the other hand, to take one more step past the positive value for you. DoubleClick.com may set a cookie that collects demographic information (age, zip code, shopping preference or any other information you share on the web), which it can then sell to advertisers. It can and will do this without your knowledge and informed consent. Moreover, you do not even have to log into DoubleClick.com for this to happen. Many sites on the web do not keep their ads or web pages themselves. Rather, they subscribe to a service that places those ads and web pages for them. When your browser requests the page from the site you are visiting, a request is made to the remote service to furnish you with the graphics for that web page. A cookie can easily be sent along with the graphics. Of course, this is done without your knowledge and informed consent.

Some people don't care about cookies. They reason that it doesn't really matter to them. Some do care (I do). So, how then do you control cookies if you care? It is not difficult.

In ***Internet Explorer 6***, click **Tools**, **Internet Options**, **General**, and press the **Delete Cookies** button. Before you do this, exit IE if you have been surfing, and restart it. Why? Cookies are held in memory until you close the browser, whereupon they are then written to your hard disk. Open the browser afresh and then do the above to wipe any past cookies.

Now, how about controlling them in the first place? Again, go to **Tools**, **Internet Options** and then click the ***Privacy*** tab. Check the **Override Automatic Cookie Handling** so that <u>you</u> have control, not IE. Click the **Accept First Party Cookies** box if you do wish to accept them from the site you are visiting (I recommend this for a reasonable browsing experience). Click the **Block Third Party Cookies** box to prevent sites other than the site you are visiting from depositing unwanted cookies (this is my setting). I also select the **Always Allow Session Cookies** box. Session cookies are those that stay in memory while you are surfing, but are not saved to disk when you exit the browser.

If you are using ***Firefox***, click **Tools**, **Options** and **Privacy**. Check the **Accept Cookies from Sites** box, but also select **Keep until: I Close Firefox**. That means no cookies will be saved on your hard drive when you exit the browser. While you are at it, go to **Private Data** and select the **Always clear my private data when I close Firefox**. You may need to modify this a bit. Click the **Settings** bar. There you will find a list of things considered private data: ***browsing history***, ***download history***, ***saved form information***, ***cache***, ***cookies***, ***saved passwords*** *and* ***authenticated sessions***. Each one of these except possibly one should be checked. The exception is saved passwords. If you have at some time added a password to the Password Manager (by clicking Remember this Password), and you like the convenience of not having to type the password each time you visit the site, be sure that **Saved Passwords** is unchecked in the list above. It is probably OK to let Password Manager store passwords, because it encrypts them.

Cookies are an invasion of your privacy when they are placed on your machine without your knowledge and informed consent. On the other hand, they also are a technological convenience that makes your surfing less of a hassle. So, like many things in modern life, they have positives and negatives. At least you can control them, using the suggestions above or some variation of these suggestions. You decide which cookies will be saved, and for how long. You own the computer, not the web sites you visit. So long as it is you making the decisions, and not them, things are in proper balance. Make sense? Happy computing!