State of Oklahoma
Monthly Cyber Security Tips
NEWSLETTER

AUGUST 2009 **Volume 4, Issue 8**

Browser Cookies

From the Desk of CPT Jeff Elliott, Oklahoma Office of Homeland Security

Mmmm… cookies - chocolate chip and oatmeal with raisins! Cookies are one of the most popular snacks that exist today. Did you know you can get "browser" cookies almost every time you go on the Internet? These cookies help with Internet commerce, allow quicker access to web sites, or can personalize your browsing experience. However, there are some privacy and security issues to be aware of, so it is important to understand the purpose of a "browser" cookie and manage their use on your computer appropriately. This tip will help you understand what a "browser" cookie is, what it is used for and what risks might be associated with using cookies.

What's a Browser Cookie and How is it Used?

Browser cookies are simply reference files stored on your computer, just like pictures and documents. When you visit a web site, the visited web site will often place a cookie on your computer. Cookies do not contain active content (executables) or links, just text-based information. The information in the cookie might indicate how often you visit the site, what kind of products you bought, what kind of things you searched for, etc.

There are two different types of browser cookies that are stored on your computer – session and permanent cookies. Session cookies are stored in the computer's memory only during your browsing session and are automatically deleted from your computer when the browser is closed. These cookies usually store a session ID that is not personally identifiable, allowing you to move from page-to-page without having to log-in repeatedly. Session cookies are never written to the hard drive and they do not collect any information from your computer. They are widely used by commercial web sites; for example, to keep track of items that a consumer has added to a shopping cart. For instance, when you add an item to your shopping cart while shopping online, the information on that item is placed into a cookie. When you are finished with your online shopping, the application then references the appropriate cookie, tallies up your purchases, and bills you for those items.

Permanent cookies are stored on your computer's hard drive and are not deleted when the browser is closed. These cookies can retain user preferences for a particular web site, allowing those preferences to be used in future browsing sessions. Permanent cookies can be used to identify individual users, so they may be used by web sites to analyze users' surfing behavior within the web site. These cookies can also be used to provide information about number of visitors, the average time spent on a particular page, log-in information stored in an account, and generally the performance of the web site.

In addition to session and permanent cookies, many sites allow their advertisers to place "third-party" cookies on your computer. Third-party cookies allow the marketing or an advertising company to track your interests and browsing through multiple web sites and companies. Third-party cookies, ones used by companies you are not dealing directly with, are more of a privacy issue than a security issue. The more you allow companies to track your online behavior, the more they can market directly to your specific interests. How cookies are processed and/or stored on your computer is controlled by your browser's privacy settings.

Risks and What Should I Do?

Although permanent cookies may be useful and convenient, there are risks associated with stored log-in credentials. Storing credentials in a cookie can increase the risk of your log-in information being discovered if someone else uses your computer or in the event your computer may be compromised. If your computer or the website you are visiting is compromised, cookies can be used for malicious purposes, such as hackers altering data in the cookie or intercepting traffic between your computer and the web site.

Is recommended that you:

Set your cookie preferences using your browser privacy settings.
Periodically delete cookies from your computer.
Session cookies should be automatically deleted when you have completed a financial transaction online. By clearing your cookies from your browser periodically you can decrease the risk of the misuse of information accidentally or intentionally stored in cookies.
Do not allow cookies to store login information.
Keep your system and browser up-to-date on patches, update your anti-spyware software, and only visit trusted web sites.
If you do not want to share your online behavior data with third-parties, set your privacy settings to not allow third-party cookies. Note, this may impact your browsing experience.
Be cautious when sharing your computer. If you stored credential information using a browser cookie (user names and password), the individual using your computer will have access to your account and will be able to process transactions in your name.

For More Information on Cookies Visit:

Web Browser Attacks: www.msisac.org/awareness/news/2008-07.cfm
Browsing Safely: Understanding Active Content and Cookies: www.us-cert.gov/cas/tips/ST04-012.html
Evaluating Your Web Browser's Security Settings: www.us-cert.gov/cas/tips/ST05-001.html
Http Cookie: http://en.wikipedia.org/wiki/HTTP_cookie
Free Security Checks: www.staysafeonline.info/content/free-security-check-ups
How to Control Cookies: www.aboutcookies.org/Default.aspx?page=1

OCTOBER IS NATIONAL CYBER SECURITY AWARENESS MONTH
"CYBER SECURITY IS OUR SHARED RESPONSIBILITY"
www.staysafeonline.org/ncsam

Live National Webcast
Security of Social Networking Sites - August 19, 2009 – 2:00pm-3:00pm EST
www.msisac.org/webcast/2009-08/index.cfm
****

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by: *http://www.msisac.org*