State of Texas
CYBER SECURITY TIPS
Monthly Newsletter

Office of the State Chief Information Security Officer | September 2009 | Volume 3, Issue 8

Browser Cookies

Mmmm… cookies – chocolate chip and oatmeal with raisins! Cookies are one of the most popular snacks ever. Did you know you can get *browser* cookies almost every time you visit the Internet? These cookies assist with Internet commerce, allow quicker access to websites, and 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 month's issue will help you understand what a *browser* cookie is, what it is used for, and what risks might be associated with using browser cookies.

WHAT'S A BROWSER COOKIE AND HOW IS IT USED?

A browser cookie is simply a reference file stored on your computer, just like pictures and documents. When you visit a website, that 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 you searched for, etc.

Two different types of browser cookies can be stored on your computer – session cookies 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 websites, 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 website, 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 websites to analyze users' web surfing behavior within the website. These cookies can also be used to provide information about the number of visitors, the average time spent on a particular page, log-in information stored in an account, and the general performance of the website.

In addition to session and permanent cookies, many sites allow their advertisers to place *third-party* cookies on your computer. Third-party cookies allow a marketing or advertising company to track your interests and browsing through multiple websites and companies. Third-party cookies, cookies 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.

WHAT ARE THE RISKS AND WHAT SHOULD I DO?

Although permanent cookies may be useful and convenient, some risks are 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 website.

Perform the following steps to protect your computer and your privacy:

- 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 websites.
- If you do not want to share your online behavior data with third parties, set your privacy settings so they do not allow third-party cookies. Note that this may impact your browsing experience.
- Be cautious when sharing your computer. If you stored credential information using a browser cookie (user names and passwords), the individual using your computer will have access to your account and will be able to process transactions in your name.

ADDITIONAL RESOURCES

For additional information on browser cookies, please 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 – **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**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.
For more information on Internet security, please visit the SecureTexas website at **www.dir.state.tx.us/securetexas**.
SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC
www.msisac.org

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM
www.us-cert.gov

Distributed by: DIR Secure Texas
www.dir.state.tx.us/securetexas