What do Cookies Do?

A cookie (called an Internet or Web cookie) is the term given to describe a type of message that is given to a Web browser by a Web server. The main purpose of a cookie is to identify users and possibly prepare customized Web pages or to save site login information for you.

When you enter a Web site using cookies, you may be asked to fill out a form providing personal information; like your name, e-mail address, and interests. This information is packaged into a cookie and sent to your Web browser, which then stores the information for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The message is sent back to the server each time the browser requests a page from the server.

A Web server has no memory so the hosted Web site you are visiting transfers a cookie file of the browser on your computer's hard disk so that the Web site can remember who you are and your preferences. This message exchange allows the Web server to use this information to present you with customized Web pages. So, for example, instead of seeing just a generic welcome page you might see a welcome page with your name on it.

Types of Cookies:

session cookie

Also called a transient cookie, a cookie that is erased when you close the Web browser. The session cookie is stored in temporary memory and is not retained after the browser is closed. Session cookies do not collect information from your computer. They typically will store information in the form of a session identification that does not personally identify the user.

persistent cookie

Also called a permanent cookie, or a stored cookie, a cookie that is stored on your hard drive until it expires (persistent cookies are set with expiration dates) or until you delete the cookie. Persistent cookies are used to collect identifying information about the user, such as Web surfing behavior or user preferences for a specific Web site.

What Information Does a Cookie Store?

For the most part a cookie will contain a string of text that contains information about the browser. To work, a cookie does not need to know where you are from, it only needs to remember your browser. Some Web sites do use cookies to store more personal information about you. However, this can be done only if you yourself have provided the Web site with that personal information. Legitimate Web sites will encrypt this personal information stored in the cookie to prevent unauthorized usage by another party with access to your cookie folder.

Cookies have six parameters that can be passed to them:

- The name of the cookie.

- The value of the cookie.

The expiration date of the cookie - this determines how long the cookie will remain active in your browser.

The path the cookie is valid for - this sets the URL path the cookie us valid in. Web pages outside of that path cannot use the cookie.

The domain the cookie is valid for. This makes the cookie accessible to pages on any of the servers when a site uses multiple servers in a domain.

The need for a secure connection - this indicates that the cookie can only be used under a secure server condition, such as a site using SSL.

What are Malicious Cookies?

Cookies normally do not compromise security, but there is a growing trend of malicious cookies. These types of cookies can be used to store and track your activity online. Cookies that watch your online activity are called malicious or tracking cookies. These are the bad cookies to watch for, because they track you and your surfing habits, over time, to build a profile of your interests. Once that profile contains enough information there is a good chance that your information can be sold to an advertising company who then uses this profile information to target you with interest specific adverts. Many antivirus programs today will flag suspicious spyware or adware cookies when scanning your system for viruses.

Viewing & Removing Cookies

Cookies are stored by the Web browser on your system's hard drive, and you can view them to see which Web sites that you visit are associated with your cookie files.

If using Internet Explorer, for example you select Tools then choose Internet Options. On the general tab you will see a section titled Browser History. Click Settings then choose View Files.

This will open up a Windows Explorer window that lists all your temporary Internet files, including your cookies. Each cookie will be identified by a site URL making it easy to determine which cookies you trust and want to keep and which you don't recall from visiting a Web site and would delete.

To change your cookie settings, simply to go back into Tools then choose Internet Options. On the Privacy tab you will see a slider bar which you can move to adjust the level at which your browser accepts cookies. Low for example blocks third-party cookies that do not have a compact privacy policy and restricts third-party cookies that save information that can be used to contact you without your consent. Medium High will do the same but also block first-party cookies that save information about you. Other privacy options you can choose would be to accept all cookies or to block all cookies as well.

If you're using a browser other than Internet Explorer, you can visit the following cookie pages on each browser Web site to find out how to manage your cookies when using Firefox, Opera, or Safari.

Firefox: Firefox Help: Firefox's Cookie Options

Opera: Security, Privacy and Cookies in Opera

Safari: Safari Help Managing cookies

First and Third-Party Cookies

When choosing a privacy setting in your browser, two terms you will see are "first-party cookies" and "third-party cookies". First party cookies are those cookies that originate from (or be sent to) the Web site you're currently viewing. These types of cookies usually will contain information about your preferences for that particular Web site. These cookies are usually Third-party cookies originate from (or will be sent to) a Web site that is not the site you are visiting. For example, if the Web site you are on using third-party advertising those third-party advertising Web sites may use a cookie to track your Web habits for marketing purposes.

While some may simply choose to block all cookies, it can make Web surfing difficult if you do this. For example if you shop online, many e-commerce shopping carts that have been implemented with cookies will not work. Sites you frequently visit which enable you to personalize content also will not show your preferences when you visit if you delete or disable that cookie.

Most cookies, despite some misconceptions, are legitimate files and will not invade your privacy. Once you get in the habit of reviewing the cookies associated with your browser and manage them on your own by way of deleting malicious cookies or trying different browser privacy settings, you can still keep the good cookies that make surfing a breeze, yet keep the bad cookies that may be tracking your surfing habits off your system.