Internet Cookies

Internet cookies have been around since the modern version of the World Wide Web, dating back to the early 1990s. What are they? What do they do? Are they a security risk? Let's answer those questions with a quick overview.

What are internet cookies?

Cookies are small files of text that allow websites and web browsers to communicate with each other. They are a fundamental part of browsing the internet that help websites function properly.

What is their purpose?

Their main purpose is to identify the user and remember various settings for the next time the user visits. For example, if you ask a site to remember your username, that information is stored in a cookie. Online shopping carts are another example. When you save an item to your cart, that item will remain there even if you close the browser.

Are there different types of cookies?

There are three notable types of cookies:

1. *Session cookies: temporary cookies that are usually deleted when you close a window or a browser*

2. *Persistent cookies: long-term cookies that store user preferences, such as your username and language choice*

3. *Third-party cookies: data-tracking cookies that store user activity, often for advertising and targeted marketing*

Where are cookies stored?

Most cookies are stored on the local hard drive of your computer. The web browser creates a folder or a file that it references every time you revisit a website. Some browsers create multiple cookie files, while others store one file for all cookies.

Are cookies a threat to security?

Cookies themselves are harmless. However, it is possible for attackers to find website vulnerabilities and exploit them to steal or manipulate cookies. There are also privacy concerns regarding internet habits. Third-party cookies store and track various data about users, which is how you end up seeing targeted advertisements for products and services.

How to enjoy cookies safely:

- *Never allow websites to store your passwords. The risk of that function outweighs the convenience.*

- *Be selective. Many websites now ask users to allow or reject cookies. Some even have an option to only allow cookies for functional purposes, which is generally the best choice.*

- *Browse in incognito mode. Some web browsers allow you to turn on incognito or private mode. By default, this blocks all cookies and trackers.*

- *Occasionally delete cookies. In the security and privacy settings of the browser, you can ask it to clear cache and delete cookies. It's never a bad idea to routinely remove cookies from your computer.*

- *Keep your browser updated. On personal devices, consider enabling automatic updates so you never miss a vital security patch. At work, always follow policy for how and when to apply updates.*

SAC the security awareness COMPANY