The ultimate guide to web cookies

Imagine a situation like this: You want to watch your favorite movie or shop online, and the minute you enter the website, a banner pops out on your window. Sounds familiar, right? This banner is actually a cookie, and if you are wondering what all the fuss about them is, you are not alone. A common misconception is that they are small programs which search for your personal information, steal the data and harm you and your business. However, cookies are actually an important browser feature and without them, most of the sites would not function.

What are web cookies?

Cookies (also known as web cookies, browser cookies or HTTP cookies) are small pieces of information in the form of a text file, containing a string of letters and numbers. This file is sent from a website to the person's browser where they are being saved before going back to the same website. Each cookie is unique in its own way and can't pass viruses or capture personal information on your computer. It enables the websites to work more efficiently, recognizing and remembering certain information, such as log-in details. Cookies are very common, and you probably have thousands of them stored right now on your computer.

How did web cookies get their name?

The "term" cookie was first coined in 1994 by the Netscape team of developers who were trying to figure out how to solve the problem of online shopping. They were trying to find a way how certain websites could "remember" the customer's personal data and items they want to buy. One tiny text file stored on a user's computer could solve this problem. The term itself is an allusion to the Fortune Cookie, a Unix application that produced different messages (or fortune) each time when they start. Since then, cookies have become an integral part of user's web browsers.

What do web cookies look like?

Each cookie has its own attributes, meaning the name, value, and the expiration date. While some websites can only store 20 cookies, browsers limit a single cookie to only 4096 bytes (4KB). A cookie containing your log-in details could look like this:

```
# Recorded 2019-01-12
username=Matt
password=Damon123
frames=yes
```

The common method used by websites to inform the visitor of the use of cookies is by putting a banner at the top and bottom, in the middle or on the sides of a webpage. So, for example, on the site Houstonpress.com, the banner is placed at the bottom of the page and reads like this:

We use cookies to collect and analyze information on site performance and usage and to enhance and customize content and advertisements. By clicking 'X' or continuing to use the site, you agree to allow cookies to be placed. To find out more, visit our cookies policy and our privacy policy.

What are cookies used for?

Cookies are used to deliver different types of information from the user's browser to the website he is visiting. That being said, there are many different reasons why a website is using cookies, such as:

1. Session management, a process of securely carrying your information through various sessions, e.g. shopping cookies identify and store your information so you don't need to enter your USERNAME and PASSWORD each time you shop an item.
2. Personalization, storing user data such as age, gender, location, interests and preferred theme, layout, font size or similar data. Facebook and Twitter use cookies to offer "LIKE" or "SHARE" on their wall.
3. Tracking users and their behavior on websites, search engines, or social media, to compile this data and create statistics about how people use their site. The collected data won't be shared with others, and their main purpose is to target audience groups according to variables. Google Adwords and Google Analytics use tracking cookies to collect data to analyze how users use the website.

Cookies also store your IP address, the version of your operating system, and your type of browser. Some of the most profitable companies across the world using cookies are Apple, Coca Cola, Microsoft, and others.

Different types of cookies

According to its main attributes, there are several types of cookies:

1. Session cookies or temporary/transient cookies are used to store temporary information. The information is acquired through one session or the time between the opening and closing of your browser. Once you leave the site and close your browser, they are deleted.

Their purpose is to connect the actions you have performed on the website, for example, to remember the items you have placed in your online shopping cart.

2. Permanent cookies are also called persistent cookies. In contrast to session cookies, permanent cookies are not deleted once you close your browser but they stored on your hard drive until the expiration date or once you delete them. They are used to remember, for example, log-in details (username and password), to avoid entering them every time you visit a particular site.
3. First-party cookies, where the term "first party" means getting cookies directly from the website's domain. What does it mean actually is that cookies are issued by the website you are on. For example, once you land on the website forbes.com, this website automatically creates a cookie which is saved on your computer.
4. Third-party cookies are related to external domains, and they are not issued by the main website. For example, if you visit the website nytimes.com, you'll get a first-party cookie issued by the website. However, the website may have a YouTube video on one of the pages which issues a third-party cookie, serving for online advertising. It may also display different types of ads, to gain more traffic and attract customers.

Where are cookies stored?

A web server doesn't have its own memory, so a cookie file needs to be stored somewhere else. The text file is placed on your hard drive through your browser, and depending on your browser, the location may be C:\WINDOWS\COOKIES or C:\WINDOWS\PROFILES\COOKIES. The next time you visit that website, your browser will send the cookie to the website's server, allowing the server to use the saved information.

How long do cookies last?

Together with its name and value, each cookie has an expiration date. Session or temporary cookies are deleted once you close your browser. However, other cookies have a specific time of expiry in the form of time and date. If the website doesn't set the expiry date, the browser will delete the cookie once it's closed. The average time of the cookie expiration is one to two years, but cookies can last for 30 or 40 years. The longest period of expiration is nearly 8000 years.

Who can access and view my cookies?

The location of cookies is directly connected to the website's domain, which means that only the server that put the cookies on your hard drive can view them and have access. They can't be accessed or examined by other websites. Accepting a cookie doesn't mean your personal information is in danger or that a cookie can deliver you a virus. Only the website that created the cookie can view and read it. However, advertising and tracking networks may use cookies to track your visits across the internet. So, for example, if you searched for a new house and later entered a website with news, you may see ads for houses on this website.

Can websites track me using cookies?

Standard websites which don't use cookies for advertising purposes have no intention of tracking your information. Tracking cookies are typically used for retargeting and advertising purposes, and they are used by third-party websites tracking your web habits. Resources that use cookies for tracking are advertisements, web analytics, and social media. Two types of tracking cookies which may have some harmful effects on your privacy are:

- **Supercookies**, which are tied to top-level domains such as ".org" and ".com". While other types of cookies are associated with specific domains such as "google.com", supercookies have much more freedom to access and change your personal information. However, most of the browsers block supercookies due to potential security concerns.
- **Zombie cookies**, which are recreated using the Quantcast technology the moment after you delete them. They are much harder to find and track, and they can follow your activity across different browsers. To completely remove them from your hard drive, you need to delete the flash cookie that recreates these zombie cookies. Modern browsers have the option to delete flash/zombie cookies through Privacy settings.

Are cookies safe?

Cookies are used via HTTP protocol, the secure protocol that encrypts the information so that they are less likely exposed to any kind of theft. They aren't malicious by nature and won't invade your privacy. Remembering your log-in details is purely for the purpose of easily managing your account. So if you clear the cookies, you'll be logged out of all of your accounts online and the settings won't be saved. Most of the browsers contain privacy settings, allowing you to review and manage cookie files. Bad cookies that are tracking your web habits can be easily put off your system.

Why do I see alerts about the use of cookies on some websites?

When cookies first appeared on the websites, most of the users had no idea what it means to have a pop-up window warning for cookie policies. Because cookies store and remember personal data, these actions needed to be under certain supervision. Currently, the European Union companies and companies that do business in Europe must be in compliance with two laws regulating the use of cookies:

- EU Cookie Directive or the Directive on Privacy and Electronic Communications (codified in 2002) states that websites need to get the user's permission before saving information in a cookie file and inform their users of the cookies usage.
- GDPR or General Data Protection Regulation (issued in May 2018) covers personal data regulations. Any information that can be related to a real, identifiable person is protected and can't be used without the person's permission (information such as the cookie identifier, IP address, and the device's ID).

Since cookies are used by companies all over the world, they had to put a "cookie warning" to keep their website's functionality.

Can cookies be blocked or deleted?

Cookies allow users to access some of the website's essential features and limiting their function can cause a lot of annoyances, such as seeing the same pop-ups and re-entering log-in details each time you visit a website. However, modern browsers (Internet Explorer, Chrome, Firefox, Microsoft Edge, Opera, Safari) allow you to manage cookies and set your tolerance. Some of the options include:

- To accept (enable) or always block (disable) cookies,

- To view them and selectively accept or delete them via cookie manager,

- To delete all cookies.

Most browsers are initially configured to accept cookies, so it's up to you to change your internet browser settings. You can also choose to be notified each time when a new cookie wants to be stored on your hard drive. Each website has its own cookie policy and reading them may provide additional information and help you decide whether or not to allow or block cookies on your computer.