

7 kinds of browser cookies you need to know

However, not all cookies are the same. In fact, there are many different types of cookies. Some types are good cookies, others are bad cookies. Let's take a closer look through the following article!

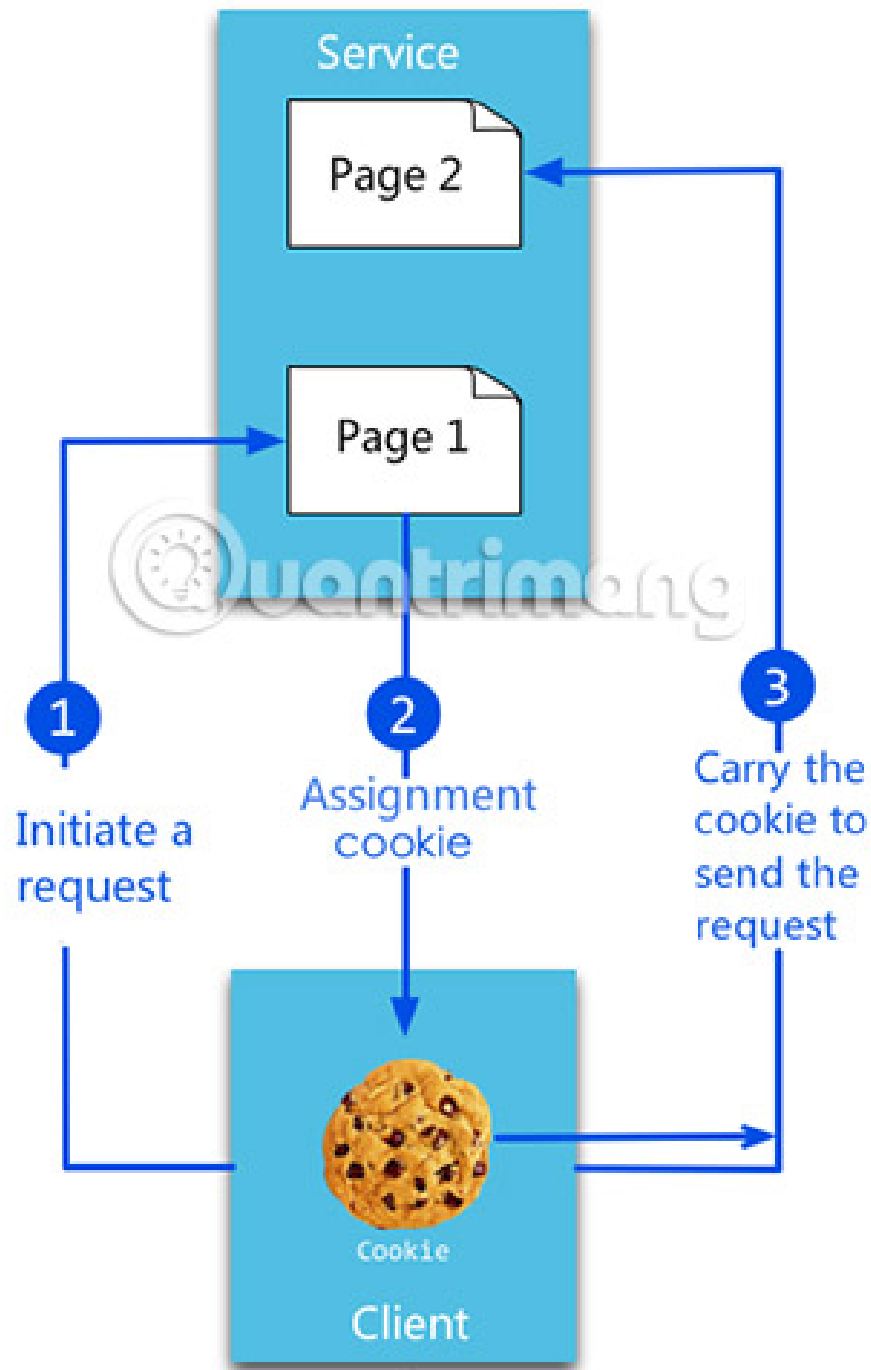
Since the EU vote in 2012 to issue mandatory cookie warnings, they always haunt the user's mind.

However, not all cookies are the same. In fact, there are many different types of cookies. Some types are good cookies, others are bad cookies. Let's take a closer look through the following article!

7 types of browser cookies most popular

1. Cookie Session
2. First-party cookies
3. Third-party cookies
4. Cookie Secure
5. HTTP-Only cookie
6. Cookie Flash
7. Cookie Zombie

1. Cookie Session



Imagine you're shopping on Amazon. You must remember all items you want to buy when browsing the website. There are no Cookie Sessions (session cookies), which will not be possible.

The easiest way is to consider session cookies as a short-term memory of a website. They allow websites to 'recognize' you when you move from one page to another in the same domain. If there is no session cookie, you will be treated as a new visitor, each time you click on a new internal link.

Session cookies do not collect any information about the computer and do not contain any personally identifiable information that can link a session to a specific user.

Session cookies are temporary. When closing the browser, your computer will automatically delete all session cookies.

2. First-party cookies

Also known as persistent cookies, permanent cookies and stored cookies, the First-Party Cookie (first-party cookie) closely resembles a website's long-term memory. They help websites remember user information and settings when they visit them again in the future.

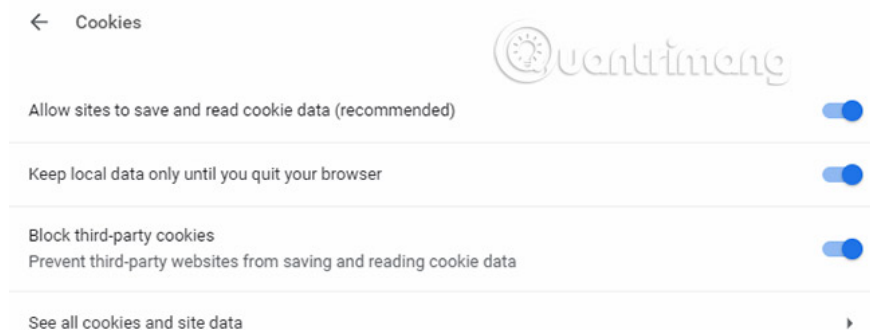
Without these cookies, websites will not be able to remember options such as setting menus, themes, selecting languages and bookmarks (bookmarks) internally between sessions. With a first-party cookie, you can make the above selections on your first visit and they will be maintained until the cookie expires.

Most cookies of this type expire after one or two years. If you do not access the website within the above time frame, the browser will automatically delete cookies. However, users can also remove them manually.

First-party cookies also play an important role in user authentication. If you have disabled them, you will need to re-enter your login information each time you visit a website.

On the downside, companies can use this type of cookie to track users. Unlike session cookies, they record information about users' browsing habits during the entire time they are activated.

3. Third-party cookies



Cookie Third-Party are bad cookies. The fact that this type of cookie has such a bad reputation for Internet users has its reasons.

For first-party cookies, the cookie's domain will match the domain of the site the user is accessing. However, third-party cookies are derived from another domain.

Since it does not come from the site the user is accessing, third-party cookies do not provide any benefits such as session cookies and first-party cookies mentioned above.

Instead, the sole purpose of third-party cookies is to track users. Tracking can take many forms. Cookies can learn about browsing history, online behavior, demographics, user spending habits, and more.

Thanks to this tracking capability, third-party cookies have become the favorite of ad networks, in order to increase sales and the number of times users visit their site.

Today, most browsers provide a simple way to block third-party cookies. The article recommends that you take these steps on the browser you're using to keep it safe while browsing the web.

If using Chrome, go to **More> Settings> Advanced> Privacy and Security> Content Settings> Cookies> Block Third-Party Cookies** .

For Mozilla Firefox browser, please refer to the article: [How to block tracking cookies on Firefox](#) to know how to do it.

4. Cookie Secure

The three types of cookies that the article mentioned so far are the most popular. But there are a few other types of cookies that users should know.

The first is Cookie Secure (security cookie). It can only be transmitted over an encrypted connection, usually HTTPS.

As long as the 'Secure' attribute of this cookie is still in effect, the user will not be able to pass the cookie over an unencrypted channel. If there is no such security property, the cookie will be sent in writing that anyone can read, so it may be blocked by unauthorized third parties.

However, even if the security factor is guaranteed, developers should not use cookies to store sensitive information. In fact, the 'Secure' attribute only protects the security of cookies. Network attackers can override security cookies from an unsecured connection. This is especially true if a site has both HTTP and HTTPS versions.

5. HTTP-Only cookie

Security cookies are usually HTTP-Only Cookies (HTTP-only cookies). Two 'Secure' and 'HTTP-only' properties work in tandem to help reduce the impact of a cross-site scripting (XSS) attack on cookies. XSS is an attack technique that forces a website to display malicious code, then these codes will be executed on the user's web browser.

In an XSS attack, a hacker will transmit malicious code to trusted sites, forcing the site to display malicious code, then the code will be executed on the user's web browser. A browser cannot tell the user which script is unreliable. Therefore, the script can access browser data about malicious websites, including cookies.

A security cookie cannot be accessed by programming languages ??(like JavaScript), so it cannot protect itself against such attacks.

6. Cookie Flash



Flash cookies are the most popular super cookies. A super cookie performs many of the same functions as regular cookies, but they are harder to find and delete.

In the case of Flash cookies, developers use the Flash plugin to hide the browser cookie's original cookie management tools.

Flash cookies are available for all browsers (so using a browser for credit card accounts and another browser to download torrents will have negligible security benefits). Flash cookies can contain 100KB of data while HTTP cookies are only about 4KB.

7. Cookie Zombie



Zombie cookies are closely linked to Flash cookies. A zombie cookie can re-create itself immediately after someone deletes it. Reproduction can be done by copies stored outside of the browser's regular cookie directory, usually the **Flash Local Shared Object** or **HTML5 Web Storage**.

The reconstruction is based on Quantcast technology. Because the Flash cookie stores a unique user ID in the storage directory of the Adobe Flash player, Quantcast can re-apply it to the new HTTP cookie if the old cookie is deleted.

It is important to remember that not all cookies are bad. Without them, the web will not work in the way we expect.

However, knowing how to manage cookies is an essential part of keeping online safe.

Good luck!

See more:

1. Delete cookies in popular browsers
2. Cookie in PHP
3. How to delete cache and cookies on Chrome, Firefox and Coc Coc

You finished reading the article "**7 kinds of browser cookies you need to know**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.