COOKIES WILL STREAMLINE YOUR WEB EXPERIENCES

Websites use cookies to streamline your web experiences. Without cookies, you'd have to login again after you leave a site or rebuild your shopping cart if you accidentally close the page, thus making cookies an important part of the internet experience. You'll want to understand why they're worth keeping — and when they're not.

Here's how cookie are intended to be used:

Cookies let websites recognize users and recall their individual login information and preferences, such as sports news versus politics.

Customized advertising is the main way cookies are used to personalize your sessions. You may view certain items or parts of a site, and cookies use these data to help build targeted ads that you might appreciate.

Shopping sites use cookies to track items users previously viewed, allowing the sites to suggest other goods they might like and keep items in shopping carts while they continue shopping.

Cookies that relate to you are stored **on your device** and not stored on a website's servers.

What are the different types of Cookies?

With a few variations, cookies in the cyber world come in two types: session and persistent.

Session cookies are used only while navigating a website. They are stored in your computer's random access memory and are never written to your hard drive. When the session ends, session cookies are automatically deleted.

Persistent cookies remain on your computer indefinitely, although many include an expiration date and are automatically removed when that date is reached.

Persistent cookies are used for two primary purposes:

Authentication. These cookies track whether a user is logged in and under what name. They also streamline login information, so users don't have to remember site passwords.

Tracking. These cookies track multiple visits to the same site over time. Some online merchants, for example, use cookies to track visits from particular users, including the pages and products viewed. The information they gain allows them to suggest other items that might interest visitors. Gradually, a profile is built based on a user's browsing history on that site.

Why Cookies Can Be Dangerous

Since the data in cookies doesn't change, cookies themselves aren't harmful.

They can't infect computers with viruses or other malware. However, some cyberattacks can hijack cookies and enable access to your browsing sessions.

The danger lies in their ability to track individuals' browsing histories. To explain, let’s discuss what cookies to watch out for.

First-Party vs. Third-Party Cookies

Some cookies may pack more of a threat than others depending on where they come from.

First-party cookies are directly created by the website you are using. These are generally safer, as long as you are browsing reputable websites or ones that have not been compromised.

Third-party cookies are more troubling. They are generated by websites that are different from the web pages users are currently surfing, usually because they're linked to ads on that page.

Visiting a site with 10 ads may generate 10 cookies, even if users never click on those ads.

Third-party cookies let advertisers or analytics companies track an individual's browsing history across the web on any sites that contain their ads.

Consequently, the advertiser could determine that a user first searched for running apparel at a specific outdoor store before checking a particular sporting goods site and then a certain online sportswear boutique.

Allowing or Removing Cookies

Cookies can be an optional part of your internet experience. If you so choose, you can limit what cookies end up on your computer or smart phone.

If you allow cookies, it will streamline your surfing. For some users, no cookies security risk is more important than a convenient internet experience.

Here’s how to remove cookies:

Before removing cookies, evaluate the ease of use expected from a website that uses cookies. In most cases, cookies improve the web experience, but they should be handled carefully.

Find the cookie section: in Edge under Settings > Cookies and Site Permissions> Manage and delete cookies and site data> see all cookies and site data > remove third-party cookies.

If you don’t want cookies, you can simply check the **remove all** box.

Removing cookies can help you mitigate your risks of privacy breaches. It can also reset your browser tracking and personalization.

Removing normal cookies is easy, but it could make certain web sites harder to navigate. Without cookies, Internet users may have to re-enter their data for each visit.

In the future, you can anonymize your web use by using a virtual private network (VPN). These services tunnel your web connection to a remote server that poses as you. Cookies will be labeled for that remote server in another country, instead of your local computer.