What are Cookies?

Everyone has seen the website banners that ask you if you'll allow cookies on your browser or not. But what exactly does this mean and what are these cookies? Well, to begin with, they are essential to the modern internet experience. A necessary part of browsing the web, cookies help web developers give you a more personal and convenient website visit. In short, cookies let websites remember you, your logins, shopping carts and more. But they can also be a treasure trove of private info and a serious vulnerability to your privacy.

Guarding your privacy online can be overwhelming. Fortunately, even a basic understanding of cookies can help you keep unwanted eyes off your internet activity. Whilst most cookies are perfectly safe, some can be used to track you without your consent by cybercriminals. In this article, we will guide you through how cookies work and how you can stay safe online.

What Are Internet Cookies?

Cookies (often known as internet cookies) are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a network. Specific cookies are used to identify specific users and improve their web browsing experience. Data stored in a cookie is created by the server upon your connection. This data is labeled with an ID unique to you and your computer. When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve you.

Due to international laws, such as the EU's General Data Protection Regulation (GDPR), and certain state laws, like the California Consumer Privacy Act (CCPA), many websites are now required to ask for permission to use certain cookies with your browser and provide you with information on how their cookies will be used if you accept.

Magic Cookies and HTTP Cookies

All cookies generally function in the same way, but have been applied to different use cases:

Magic cookies are an old computing term that refers to packets of information that are sent and received without changes to the data. This would commonly be used for a login to computer database systems, such as a business internal network. This concept predates the modern "cookie" we use today.

HTTP cookies are a repurposed version of the "magic cookie" built for contemporary internet browsing. In 1994, web browser programmer Lou Montulli used the "magic cookie" as inspiration to create the HTTP cookie, whilst he was helping an online shopping store fix their overloaded servers. The HTTP cookie is what we currently refer to as a cookie more generally today. It is also what some cybercriminals can use to spy on your online activity and hack your personal information.

What are HTTP Cookies?

HTTP cookies, or internet cookies, are built specifically for web browsers to track, personalize and save information about each user's session. A "session" is the word used to define the amount of time you spend on a site. Cookies are created to identify you when you visit a new website. The web server — which stores the website's data — sends a short stream of identifying information to your web browser in the form of cookies. This identifying data (known sometimes as "browser cookies") is processed and read by "name-value" pairs. These

pairs tell the cookies where to be sent and what data to recall.

So, where are the cookies are stored? It's simple: your web browser will store them locally to remember the "name-value pair" that identifies you. When you return to the website in the future, your web browser returns that cookie data to the website's server, triggering the recall of your data from your previous sessions.

To put it simply, cookies are a bit like getting a ticket for a coat check:

- **You hand over your "coat" to the cloak desk.** You connect/visit a website and a pocket of data is linked to you on the website's server. This data can be your personal account, your shopping cart or even just what pages you've visited.
- **You get a "ticket" to identify you as the "coat" owner.** The cookie (containing the data) is then given to you and stored in your web browser. It has a unique ID especially for you.
- **If you leave and return, you can get the "coat" with your "ticket".** When you revisit the website, your browser gives the website the cookie back. The website then reads the unique ID in the cookie to assemble your activity data, bringing you back to where you were when you first visited, as if you never left.

What Are Cookies Used For?

Websites use HTTP cookies to streamline your web experiences. Without cookies, you'd have to login every time you leave a site or rebuild your shopping cart if you accidentally closed the page. Making cookies is an important part of the modern internet experience.

To be more concise, cookies are intended to be used for:

1. **Session management:** For example, cookies let websites recognize users and recall their individual login information and preferences, such as sports news versus politics.
2. **Personalization:** 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 this data to help build targeted ads that you might enjoy. They're also used for language preferences as well.
3. **Tracking:** 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 on another part of the

website. They will also track and monitor performance analytics, like how many times you visited a page or how much time you spent on a page.

While this is mostly for your benefit, web developers get a lot out of this set-up as well. Cookies are stored on your device locally to free up storage space on a website's servers. In turn, websites can personalize content, whilst saving money on server maintenance and storage costs.

What are the different types of HTTP Cookies?

With a few variations (which we'll discuss later), cookies in the cyber world essentially come in two types: session cookies and persistent cookies.

Session cookies are used only while navigating a website. They are stored in random access memory and are never written on to the hard drive. When the session ends, session cookies are automatically deleted. They also help the "back" button work on your browser.

Persistent cookies, on the other hand, remain on a 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:

1. **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.
2. **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.

First-Party vs. Third-Party Cookies

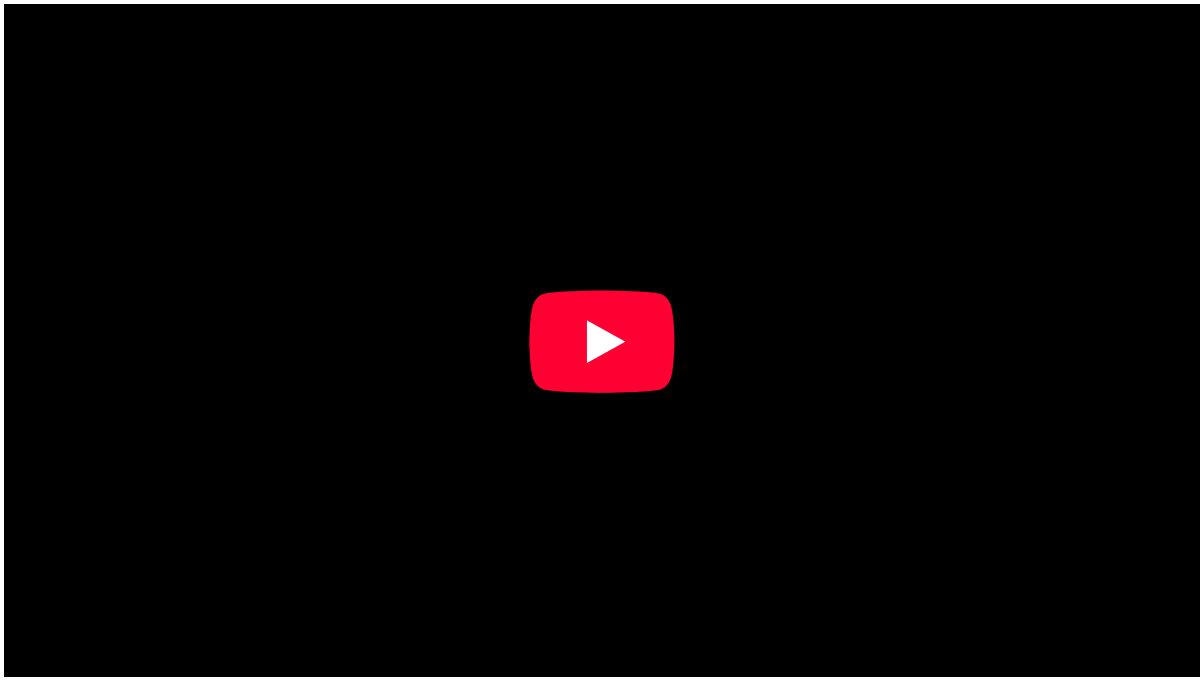
From here, internet cookies can be broken down into two further categories: first-party and third-party. Depending on where they come from, some cookies may potentially be more of a threat than others.

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 by a recent data breach or cyberattack.

Third-party cookies are more troubling. They are generated by websites that are different from the pages that the users are currently surfing, usually because they're linked to ads on that page. Third-party cookies let advertisers or analytics companies track an individual's browsing history across the web on any sites that contain their ads. However, as previously mentioned, due to new data protection laws, allowing third-party cookies to access your browser is now optional in many countries and states. These days, most third-party cookies have no direct impact on your browsing experience, as many browsers have already begun phasing them out (Google has announced the end of third-party cookies in Chrome by 2024). Many websites still operate fine and remember your preferences without using third-party cookies.

Zombie cookies are a form of third-party, persistent cookie, which are permanently installed on users' computers. They have the unique ability to reappear after they've been "deleted" from your computer. They are also sometimes called "flash cookies" or "supercookies" and are extremely difficult to remove. Like other third-party cookies, zombie cookies can be used by web analytics companies to track unique individuals' browsing histories. Websites may also use zombies to ban specific users. In some cases, however, these types of cookies can be fabricated by hackers and used to infect your system with viruses and malware.

Essential Cookies are now synonymous with the pop-up asking you for your cookie preferences when you first visit a website. Essential cookies are first-party session cookies that are necessary to run the website or services you have requested online (such as remembering your login credentials).



Enabling and Removing Cookies

Some cookies can be an optional part of your internet experience, for example you can limit what cookies end up on your computer or mobile device. Today, this is commonly done when you visit a website and are given the option to enable third-party (or other) cookies or not.

If you enable and allow cookies, it can streamline your web-surfing experience. Here's how to allow cookies:

- Find the cookie section — typically under Settings Privacy.
- Click the boxes to allow cookies. Sometimes the option says, allow "local" data.
- If you don't want cookies, you can simply uncheck these boxes.

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. Different browsers store cookies in different places, but usually, you can:

- Find the Settings, Privacy section — sometimes listed under Tools, Internet Options, or Advanced.
- Follow the prompts on the available options to manage or remove cookies.

However, to remove persistent tracking cookie infestations and more malicious types created by hackers, you'll want to enlist the help of some Premium Protection. In the future, you should also 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 then be labeled for that remote server in another country, instead of your local computer.

Regardless of how you handle cookies, it's best to remain on guard and clean up your cookies often.

Related articles:

- What is Internet Security?

Recommended products:

- Kaspersky Safe Kids
- Kaspersky Home Security
- Kaspersky Password Manager

Share with your friends

Related articles

What is Quishing? How to protect yourself from QR code phishing

Learn about QR code phishing, including the...

Read More ›

What is ethical hacking?

Ethical hackers can be useful for organizations...

Read More ›

Home Solutions

Kaspersky Standard

Kaspersky Plus

Kaspersky Premium

Kaspersky Safe Kids

Kaspersky VPN Secure Connection

Kaspersky Password Manager

All Solutions

Device Specific Solutions

Android Antivirus

Mac Antivirus

Mobile Security

Windows Antivirus

Linux Antivirus

VPN for Windows

VPN for Android

VPN for iPhone

VPN for Routers

Small & Medium Business

Kaspersky Small Office Security

Kaspersky Next EDR Foundations

Kaspersky Next EDR Optimum

Kaspersky Next XDR Optimum

Kaspersky Next MXDR Optimum

All Products

Enterprise Solutions

Kaspersky Next

Cybersecurity Services

Kaspersky MDR

Kaspersky Next XDR Expert

Kaspersky Threat Intelligence

Hybrid Cloud Security

Hybrid Cloud Security

All Solutions