What are Cookies?

HTTP cookies are essential to the modern Internet but a vulnerability to your privacy. As a necessary part of web browsing, HTTP cookies help web developers give you more personal, convenient website visits. Cookies let websites remember you, your website logins, shopping carts and more. But they can also be a treasure trove of private info for criminals to spy on.

Guarding your privacy online can be overwhelming. Fortunately, even a basic understanding of cookies can help you keep unwanted eyes off your internet activity.

In this article, we will guide you through how cookies work and how you can stay safe online. We'll answer key questions like:

- What are cookies?
- What are cookies on a computer?
- What are cookies on a website?
- Can cookies contain viruses?
- How can I remove cookies?

What Are Cookies?

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 computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your 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 to you.

Different types of cookies - Magic Cookies and HTTP Cookies

- Magic Cookies
- HTTP Cookies

Cookies generally function the same but have been applied to different use cases:

This concept predates the modern "cookie" we use today.

HTTP cookies are a repurposed version of the "magic cookie" built for internet browsing. Web browser programmer Lou Montulli used the "magic cookie" as inspiration in 1994. He recreated this concept for browsers when he helped an online shopping store fix their overloaded servers.

The HTTP cookie is what we currently use to manage our online experiences. It is also what some malicious people can use to spy on your online activity and steal your personal info.

To explain, you'll want to understand exactly what are internet cookies and why do they matter?

What are HTTP Cookies?

HTTP cookies, or internet cookies, are built specifically for Internet web browsers to track, personalize, and save information about each user's session. A "session" just refers to the 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 info to your web browser.

Browser cookies are identified and read by "name-value" pairs. These tell cookies where to be sent and what data to recall.

The server only sends the cookie when it wants the web browser to save it. If you're wondering "where are cookies stored," it's simple: your web browser will store it locally to remember the "name-value pair" that identifies you.

If a user returns to that site in the future, the web browser returns that data to the web server in the form of a cookie. This is when your browser will send it back to the server to recall 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.** In this case, a pocket of data is linked to you on the website server when you connect. This data can be your personal account, your shopping cart, or even just what pages you've

web browser. It has a unique ID especially for you.

- **If you leave and return, you can get the "coat" with your "ticket".** Your browser gives the website your cookie. It reads the unique ID in the cookie to assemble your activity data and recall your visit just as you left it.

What Are Cookies Used For?

Websites use HTTP 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. Making cookies an important a part of the internet experience.

Based on this, you'll want to understand why they're worth keeping — and when they're not.

Here's how cookie are intended to be used:

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.
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.

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 while saving money on server maintenance and storage costs.

What are the different types of HTTP Cookies?

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

When the session ends, session cookies are automatically deleted. They also help the "back" button or third-party anonymizer plugins work. These plugins are designed for specific browsers to work and help maintain user privacy.

Persistent cookies 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.

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.

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.

Zombie cookies are from a third-party and permanently installed on users' computers, even when they opt not to install cookies. They also reappear after they've been deleted. When zombie cookies first appeared, they were created from data stored in the Adobe Flash storage bin. They are sometimes called “flash cookies” 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.

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 mobile device.

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 allow cookies:

- Find the cookie section — typically under Settings > Privacy.
- Click the boxes to allow cookies. Sometimes the option says, "Allow local data.”

personalization. To help, Kaspersky offers step-by-step instructions for removing cookies from the most popular web browsers.

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.

To remove tracking cookie infestations and more malicious types, you'll want to enlist the help of some internet security software.

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.

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.

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

Related articles:

- What is Adware?
- What is a Trojan?
- Computer Viruses and Malware Facts and FAQ
- Spam and Phishing

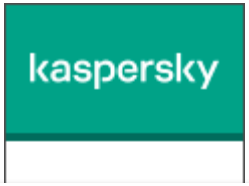
Cryptography Definition

What is an SSL certificate – Definition and Explanation

What is Jailbreaking – Definition and Explanation

What is an IP Address – Definition and Explanation

What is Facial Recognition – Definition and Explanation



Protection - PC, Mac and Mobile

Kaspersky Total Security

Learn More

Protecting You, Your Family & More

Get the Power to Protect. Discover how our award-winning security helps protect what matters most to you.

Get FREE Tools

Our FREE security tools and more can help you check all is as it should be... on your PC, Mac or mobile device.

We're Here to Help

Helping you stay safe is what we're about – so, if you need to contact us, get answers to some FAQs or access our technical support team, click here.

stay safe... online and beyond.

can get a FREE trial of one of our products – so you can put our technologies through their paces.

license or upgrade to another Kaspersky product

Stay in Touch

Home Products

Kaspersky Anti-Virus

Kaspersky Android Antivirus

Kaspersky Internet Security

Kaspersky Total Security

Kaspersky Security Cloud

Kaspersky VPN Secure Connection

Free Antivirus

All Products

Small Business Products
(1-50 EMPLOYEES)

Kaspersky Small Office Security

Kaspersky Endpoint Security Cloud

All Products

Medium Business Products
(51-999 EMPLOYEES)

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions
(1000+ EMPLOYEES)

Cybersecurity Services

Threat Management and Defense

Endpoint Security

Threat Intelligence

All Solutions

© 2021 AO Kaspersky Lab. All Rights Reserved. • Privacy Policy • Anti-Corruption Policy • Licence Agreement B2C • Licence Agreement B2B

Global