Browser Cookies: What Are They & Why Should You Care?

by Jon Penland

Last updated: February 27, 2020

Disclosure: Your support helps keep the site running! We earn a referral fee for some of the services we recommend on this page. Learn more

Cookies, more properly called HTTP cookies, are small bits of data stored as text files on a browser. Websites use those small bits of data to keep track of users and enable user-specific features.

They enable core website functionality, such as e-commerce shopping carts, and are also used for more controversial purposes, such as tracking user activity.

Cookies are a necessary part of the way the web works as well as a source of privacy concerns and security risks. For this reason, casual web users and web developers have good reason to better understand how these tiny bits of data work.

This guide provides an in-depth introduction to cookies broken into two parts:

- **A Layman's Guide to Cookies**: the basics that every internet user should know about cookies.
- **A Developer's Guide to Using Cookies**: how cookies work, how to avoid getting into legal trouble due to cookie use, and technical resources to learn more about cookies.

Ready? Let's get to it.

A Layman's Guide to Cookies

Whether you are just a casual internet user or make your living as a web developer, there are certain things about HTTP cookies that every internet user should know, such as the purpose of cookies and the privacy and security risks inherent to their use.

However, before we jump into that, let's start by answering this question: where did web cookies come from?

A Brief History of HTTP Cookies

Cookies were developed for the first time in 1994 by Lou Montulli, an employee of Netscape Communications. Along with John Giannandrea, Lou developed cookies as a solution to make e-commerce shopping carts possible.

The first actual real-world application of cookies on the web was to determine whether visitors to the Netscape website had been there previously.

Initially cookies were accepted by default by all supported browsers and very few end-users had any idea about their presence or use. That all changed in February of 1996 when the Financial Times published a piece detailing their existence, purpose, and use.

What followed was intense media scrutiny for the next few years due to the privacy risks inherent to visitor tracking.

The Internet Engineering Task Force (IETF) was given the job of coming up with a formal cookie specification that agreed with the concerns expressed by the media.

Of particular concern were the risks associated with allowing third-party cookies. These are more commonly known as tracking cookies. IETF attempted to require that third-party cookies be explicitly disallowed or only allowed after explicit user opt-in.

However, the leading browser developers at that time, Netscape and Microsoft, ignored the IETF recommendation and went along with online advertiser wishes to allow third-party tracking cookies.

The current cookie specification acknowledges the use of third-party cookies and the risks inherent to their use, but ends up placing the onus for dealing with this risk back on browser developers:

This document grants user agents (browsers) wide latitude to experiment with third-party cookie policies that balance the privacy and compatibility needs of their users.

What Goes Into a Cookie?

Cookies associate bits of data to a specific user.

For example, if you visit a website, the site may deliver a cookie identifying you as user X. If you leave the site and then return to it again, that cookie will be used by the website to recognize that you are the same user X that was at the site previously.

Cookies necessarily contain, at a minimum, two pieces of data: a unique user identifier and some information about that user.

They may also contain a wide range of attributes that tell browsers what do with the cookie — a topic we'll get into when we get to the portion of this guide oriented toward developers.

A common example of how this all works is an authentication cookie.

When you log into a website the site may return a cookie that identifies your user account and confirms that you have successfully logged in to the site. When you interact with the site it will use that cookie as confirmation that you are a logged-in user.

Common Types of Cookies

Cookies can be classified in several different ways. Let's look at four of the most common classifications to better understand how cookies are used and how they work.

Session cookies are temporary cookies stored in the browser's memory just until the browser is closed.

These types of cookies pose less of a security risk and are used to power e-commerce shopping carts, to control the page elements shown to a user during a single multi-page visit to a website, and for other short-term storage purposes.

Peristent cookies are longer-term cookies that are tagged by the issuer with an expiration date.

These cookies are stored by the browser even after the browser is closed. They are returned to the issuer every time you visit the site that issued the cookie or view a site that contains a resource (such as an ad) issued by the original cookie issuer.

In this way, persistent cookies can track your activity not only on the site that issued the cookie but also on any site that includes a resource issued by the same site. This is the mechanism sites like Google and Facebook use to create a log of user activity across multiple websites.

When you click "Remember Me" or a similar option when logging into an online account, a persistent cookie is used to store your login information on your browser.

Due to the fact that persistent cookies stick around much longer than session cookies, and can theoretically track your activity over time at multiple sites,

persistent cookies pose a greater risk than session cookies.

First-party cookies are cookies created by the site you're currently visiting. For example, while on this site we use cookies for various purposes, such as making our host filtering feature work. The cookies we issue while you're visiting our site are first-party cookies.

Third-party cookies are cookies added by a domain that is not the domain you are currently visiting. The most common use of third-party cookies is to track users who click on advertisements and associate them with the referring domain.

For example, when you click on an ad on a website, a third-party cookie is used to associate your traffic with the site where the ad appeared.

While cookies are a necessary part of the modern web, they can also pose a considerable risk of invasion of privacy as well as a security risk to the websites that use them.

User Beware: Cookie Risk and Reward

As a web user, you will want to know the risks associated with cookies and what you can do view cookies and delete them when necessary. Let's start with the risks associated with cookies which tend to fall into two categories: fraud and invasion of privacy.

Cookie Fraud

Methods of committing cookie fraud are technically complex, but it's worth knowing about them in case you ever encounter one of these exploits.

In most cases, cookie fraud takes on one of two forms: a malicious website uses legitimate website visitors as a proxy in an attack on a website or to game tracking systems by attaching false session IDs to a legitimate user's activity. Let's look at four common cookie fraud exploits to learn how they work:

- **Cross-site scripting (XSS)**: a user visits a malicious website and receives a cookie that contains a script payload targeting a different website. The malicious cookie is disguised to look like it originated from the targeted website. When the user visits the targeted site, the malicious cookie, including the script payload, is sent to the server hosting the targeted site.
- **Session fixation**: a user receives a malicious cookie that contains the cookie issuer's session ID. When the user attempts to log into a targeted domain, the issuer's session ID is logged in instead of the user's session ID. In this way, it looks to the targeted domain like the issuer is performing actions that the user is actually performing.
- **Cross site request forgery attack (XSRF)**: a user visits a legitimate site and receives a legitimate cookie. The user then visits a malicious site that instructs the user's browser to perform some action targeting the legitimate site. The legitimate site receives the request along with the legitimate cookie and performs the action since it appears to be initiated by a legitimate user.
- **Cookie tossing attack**: a user visits a malicious site that provides a cookie designed to look like it originated from a subdomain of a targeted site, such as *http://subdomain.example.com*. When the user visits the targeted site, *http://example.com* in this case, the subdomain cookie is sent along with any legitimate cookies. If the subdomain cookie is interpreted first, the data in that cookie will overrule the data contained in any subsequent legitimate cookies.

As you can see, in virtually all cases of cookie fraud, cookies are used to either falsify the identity of legitimate users or to use the legitimate user's identity to perform malicious actions.

Protecting Against Cookie Fraud

Cookies, even malicious ones, aren't viruses. The plain text nature of cookies means they cannot be executed on your computer.

So your antivirus software does little-to-nothing to protect against malicious cookies. However, there are at least two things you can do to protect yourself against becoming a victim of cookie fraud:

- Keep your browser up to date. Many cookie exploits are designed to take advantage of security holes in outdated browsers. Most browsers today update automatically, but if you happen to be using an antiquated browser, stop using it and update it.
- Avoid questionable sites. If you are ever warned either by your browser or by a search engine that a site is potentially malicious, don't proceed to the site. It just isn't worth the risk.

Invasion of Privacy

Invasion of privacy is a bigger concern than cookie fraud to many users.

If you consider how many sites have some sort of embedded Google resource — Adsense, Analytics, Maps, login with Google, and so forth — it's easy to see how Google is continually adding to an already massive dossier of cross-site activity for most web users.

Many users feel that Google's use of that information to deliver targeted ads is, at a minimum, creepy, and potentially a grave invasion of privacy.

Google is hardly alone in this regard. All web advertising platforms — from Infolinks and Revcontent to Disqus and Facebook — are constantly trying to mine more data about every user for the purpose of delivering ads with increased relevancy and improved user targeting.

In short, if you're going to use the web and allow your browser to accept cookies, you are being tracked, and now you know it.

Protect Your Privacy

There's really no way around accepting cookies. However, there are a few things you can do to limit the amount of exposure you face when it comes to cookie-initiated invasion of privacy:

- Pay attention to your browser's security and privacy settings. Open your browser's settings menu and look for the security or privacy settings. Set the cookie policies to be as stringent as you deem necessary without making it unduly difficult to access website features.
- Use Private or Incognito browsing mode. All modern browsers provide the option to browse the web using a clean cookie slate. When using this mode, the browser will not use any existing persistent cookies. When you close the browser, all cookies, even persistent ones, will be deleted. Just keep in mind that this means no passwords will be saved and every site will think it's the first time you ever visited it every time you visit it.

How to View and Delete the Cookies Stored by Your Browser

Every major browser makes it pretty easy to view and delete the cookies stored by it. However, the process varies from one browser to the next.

In general, you will want to open the browser settings and look for the privacy or security section. Next, look for an option that allows you to view the cookies stored by your browser. When viewing individual cookies you will be provided the option to delete any cookies you wish to remove from your browser. You should also find an option to easily delete all cookies if you wish to do so.

If you get stuck, just google "How to view cookies in XYZ" replacing "XYZ" with the name of your browser.

One special type of cookie you may have trouble deleting is a zombie cookie. This type of cookie is automatically recreated by a script stored outside of the browser memory every time you delete it. The result? You can't simply delete the cookie and have it stay gone for good.

This strange behavior might make you think that all zombie cookies are malicious, but that isn't the case. Some zombie cookies have legitimate uses. However, their behavior has caused them to be universally derided by both security experts and privacy advocates.

To delete these types of cookies takes a little more perseverance, and typically involves the exercise of your googling skills to figure out how others have dealt with the same undeletable cookie. What you'll have to do is figure out where the script that is recreating the cookie is stored and delete that script to stop the continual rebirth of the zombie cookie.

Cookie Control: Browsers and Devices

The good news is that you aren't entirely at the mercy of the good or bad intentions of web developers. You can be proactive and manage the cookie policy of the browsers you use. By taking the time to establish a cookie policy you can limit your exposure to some of the risks inherent to using the web.

Establishing a Browser Cookie Control Policy

Every major browser makes it pretty easy to manage cookies. However, the process does vary from one browser to the next. Let's take a look at how you can manage cookie policy in the desktop versions of Chrome, Firefox, Microsoft Edge, and Internet Explorer.

Chrome

Open the settings menu and use the *Search settings* field to search for "cookies." This will return the *Privacy* settings. You can also find this section by scrolling to the bottom of the settings menu, selecting *Show advanced settings*, and locating the *Privacy* section.

From the *Privacy* settings, select the *Content settings* option. By default, all first and third-party cookies are accepted — a setting which Chrome refers to as *Allow local data to be set (recommended)*. If you aren't happy with this policy, alternatives include:

- *Keep local data only until you quit your browser*: Select this option to accept cookies but the delete them when you exit the browser.
- *Block sites from setting any data*: Select this option to completely disable all cookies.

- *Block third-party cookies and site data*: If you don't want to allow third-party cookies, select this checkbox.
- *Manage exceptions*: Press this button to manage the list of sites that operate with a site-specific cookie policy.

Firefox

To manage cookies in Firefox open the browser menu, select *Options*, and then select the *Privacy* tab. In the *History* section, select the drop-down menu item to *Use custom settings for history*, and then select from the following options:

- Deselect the default option to *Accept cookies from sites* to completely disable cookies.
- From the *Accept third-party cookies* drop-down menu you can choose to accept all third-party cookies, only those from sites you've visited previously, or block third-party cookies entirely.
- Select the *Exceptions* button to manage a list of websites with a cookie policy different from the browser policy.
- From the *Keep until* drop-down menu, opt to keep cookies until they expire or delete them when Firefox is closed.

Edge

Managing cookies in Microsoft's newest browser is pretty straightforward. First, open the browser settings menu. Scroll to the bottom and click on *View advanced settings*. Scroll to the bottom again and you'll find a *Cookies* drop-down menu. There are three self-explanatory options available in this menu:

- *Don't block cookies* (selected by default)
- *Block all cookies*
- *Block only third-party cookies*.

Notably absent from this menu is any way to delete cookies each time the browser is closed.

However, you can make that happen by going back to the primary settings menu (click the « button at the top of the *Advanced Settings* menu).

Next, select the *Choose what to clear* button below *Clear browsing data*. Select just the *Cookies and saved website data* option, and then select the toggle to *Always clear this when I close the browser*.

Internet Explorer

Managing cookies in IE 9, IE 10, and IE 11 is handled in the same way.

First, open the *Internet Options* menu. Next, select the *Privacy* tab. From the *Privacy* tab, select the *Advanced* button. From the next menu you can establish a policy for both first-party and third-party cookies. In addition, you can select a checkbox to override the cookie policy and *Always allow session cookies*.

If you would also like to delete all cookies every time you close Internet Explorer, go back to the *General* tab and select the checkbox to *Delete browsing history on exit*. Finally, select the *Apply* button at the bottom of the *Internet Options* menu to save and apply your changes.

Managing Cookies on Your Mobile Device

Managing cookies on mobile devices can vary from the process of managing cookies in a desktop browser.

This is primarily because most mobile operating systems include a native browser. In addition, mobile browsers may not offer all of the same options as their desktop siblings, and this can further complicate matters.

Let's take a look at managing cookies on iOS, Android, and Blackberry devices.

Apple iOS

If you use Safari on iOS, you can manage cookie policy by opening the *Settings* app, scrolling down and selecting *Safari*, and then scrolling down

until you see the *Block cookies* option. The *Block cookies* menu will display four options:

- *Always block*
- *Allow from Current Website Only* (first-party cookies)
- *Allow from Websites I Visit* (default option, allows limited third-party cookies)
- *Always Allow*.

If you don't use Safari on your iPhone, there's a good chance you use Chrome instead. Chrome on iOS makes it possible to delete cookies but not to manage cookie policy.

To delete cookies open the Chrome menu and select *Settings*. Scroll down and select *Privacy*. Scroll down again and select *Clear Browsing Data*. Select the types of data you want to delete, making sure to select *Cookies, Site Data*, and then select the option to *Clear Browsing Data*.

Another option for Chrome users on iOS is to browse using an incognito tab, and make sure to close the tab prior to closing the browser. That way, no cookies will ever be stored beyond the current browsing session.

Andriod

Many Android devices ships with a built-in browser. Unfortunately, these browsers vary from one manufacturer and phone model to the next. As a result, managing cookies in these browsers varies considerably. However, in general, what you need to do is open the browser, find the settings menu, and locate the privacy settings.

Things are a little more straightforward for users of Chrome on Android. To manage cookie policy, open the browser, find the menu, and select *Settings*. Navigate to *Site Settings* and select *Cookies*. From this menu you can toggle cookie acceptance on or off, decide whether or not to *Allow third-party cookies*, and manage a list of websites excluded from the cookie policy.

Blackberry

Some of the latest Blackberry devices are powered by Android. As a result, managing cookies in those devices will fall under the Android section above. However, a few Blackberry devices do run Blackberry 10. To manage cookie policy for the built-in Blackberry 10 browser follow these steps:

- Launch the browser and open the browser menu.
- Select *Settings* and then *Privacy and Security*.
- From this menu you can toggle cookie acceptance on and off, manage a list of website exceptions, and clear all cookies.

A Developer's Guide to Using Cookies

Cookies are just text files. How hard can they be to work with? If only things were that simple.

Cookies are implemented in many different ways depending on the purpose of the cookie and the server issuing the cookie.

In this part of the guide, we'll touch briefly on implementing cookies and dive into legal issues surrounding cookie use. Finally, I'll point you towards resources you can use to learn more about the implementation of cookies and how you can leverage cookies in your web development projects.

Technical Intro to Implementing Cookies

Cookies are created when a web server tells a browser to create the cookie. The instructions for creating the cookie are usually sent in an HTTP header and look something like this:

```
Set-Cookie: <cookie_name>=<cookie_value>
```

Cookies may also be created with client-side JavaScript by using the `document.cookie` method.

Once a cookie has been created by a browser, when the browser makes a subsequent request of the same domain it will send back any cookies

belonging to that domain as part of the request.

The cookie in the example above is a session cookie. Persistent cookies are created by adding an `Expires` attribute to the `Set-Cookie` header. In addition to `Expires`, several other attributes can be used to control how browsers treat cookies:

- Cookies tagged with the `Secure` attribute will only be sent if the request from the browser is transmitted over an encrypted protocol (https).
- Cookies flagged as `HttpOnly` will be inaccessible to JavaScript within the webpage DOM and will only be transmitted back to the issuing domain.
- The `SameSite` flag is a relatively new attribute that ensures that cookies will only be transmitted back to the same website from which they originated.

Cookies and the Law

As a web developer, you need to be aware of the privacy laws and directives that affect your work. If you ignore the laws that apply to the use of cookies, you may even find yourself facing steep fines.

When it comes to using cookies, there are at least three legal issues to take into consideration:

- **EU Cookie Law**: what started out as an EU directive was later incorporated into law by every country in the EU. In short, the cookie law says that if you're based in the EU or target consumers in the EU you must get permission from users in order to use cookies.
- **FTC Disclosure Requirements**: third-party tracking for the purpose of advertising and affiliate sales is one of the primary uses of HTTP cookies. If you're using cookies for this purpose, the FTC makes clear that you must let your site visitors know what you're doing.

- **Privacy Policy Requirements**: several countries, including the United States, the UK, Australia, and every country in the EU, require that you let users know what you're doing with their personal data. If you use cookies in any way to track user activity, including using analytics cookies to track visitor traffic, you are required by law to publish a privacy policy explaining what data you collect and how you use it.

Complying with the law with regard to cookies isn't that hard. In most cases, all you need to do are follow these three guidelines:

- If you're based in the EU or targeting EU consumers, make sure that you give them the opportunity to acknowledge that your site uses cookies.
- If you allow paid advertisements or the placement of affiliate ads on your site, disclose that information on your website in an obvious manner.
- If you track user activity or collect any user data, provide a comprehensive privacy policy explaining what data you gather and how it's used.

Do those three things and you'll stay on the right side of the law. Having said that, we should also say that we aren't lawyers, we aren't providing legal advice, and if you have any specific questions about this topic you really should consult a lawyer.

Resources

The way cookies are set and used varies from one programming environment to the next. If you know how you're going to use cookies, the tutorials below will help you pinpoint the information you need to use cookies with your website or application.

- W3Schools, JavaScript Cookies Tutorial: learn how to fetch information from cookies with JavaScript and also how to set cookies using client-side scripting.
- W3Schools, PHP Cookies Tutorial: learn how to send cookies with PHP with an HTTP header and how to incorporate data from cookies into your code.
- Mozilla Developer Network, HTTP Cookies: a technical introduction to the use of HTTP cookies.
- Mozilla Developer Network, Document.cookie: a technical introduction to the use of JavaScript cookies.
- TutorialsPoint, JavaScript Cookies Tutorial: another excellent and comprehensive tutorial on using JavaScript to work with cookies.
- PHP Manual: Cookies: if you are a PHP developer, refer to the official documentation to learn how to work with cookies in PHP.
- Pontikis.net, How to Create, Read, Update and Delete a Cookie with PHP or JavaScript: a more comprehensive look at cookie use based on the two most-commonly used programming languages of the web, PHP and JavaScript.
- Hongkiat, How to Use Cookie and HTML5 localStorage: HTML5 added new strategies for storing cookies. Learn how to take advantage of these new features.
- Torque, How to Use Cookies in WordPress: as the most popular CMS on the web, it's critical that every web developer know the basics of using cookies in WordPress.
- Microsoft Developer Network, ASP.NET Cookies Overview: an introduction to cookies for ASP.NET developers.
- The Odin Project, Sessions, Cookies, and Authentication (Ruby on Rails): an introduction to cookies for Ruby on Rails developers.

- Jay Conrod, How to use HTTP cookies in Python: an introduction to cookies for Python developers.
- Oracle Java Documentation: Working With Cookies: an introduction to cookies for Java developers.

Conclusion

Cookies are an integral part of the modern web. However, they do present a bit of a double-edged sword: they enable mission-critical website features while simultaneously presenting a legitimate risk to website security and user privacy.

In the end, cookies aren't going anywhere and the vast majority of websites use cookies in some form or fashion.

By educating yourself about how cookies work and how to deal with them you'll be better prepared to take advantage of their benefits while protecting yourself against the inherent risks.

Further Reading and Resources

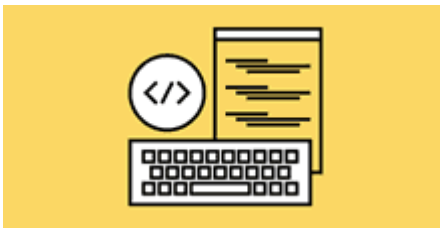
We have more guides, tutorials, and infographics related to coding and website development:

- Composing Good HTML: this is a solid introduction to writing well-formed HTML and using HTML validator software.
- CSS3 – Intro, Guides & Resources: this is a great place to start learning webpage layout.
- How to Choose the Right CMS: learn what you need in a CMS and get an overview of the top 30 CMSs.

HTML for Beginners – Ultimate Guide

If you really want to learn HTML, we've created a book-length article, HTML for Beginners – Ultimate Guide.

And it really is the ultimate guide; it will take you from the very beginning to mastery.



HTML for Beginners – Ultimate Guide

About Jon Penland

Jon has worked in many capacities in the high tech world, including engineering and development. He's written many articles for WhoIsHostingThis.com, including expert reviews of web hosts, programming resource guides, and even front-end development tutorials. He lives in Georgia with his wife and five children.

◀ Hostinger Review: We Test Their Claims, And THIS Is What We Found

How To Stop People From Stealing Your Pictures ▶

Comments

Your email address will not be published. Required fields are marked *

Share your thoughts

Name *

Email *

COMMENT

Stephen Johnson
February 6, 2020

As a baby boomer with little knowledge of the mechanics and dangers of the IT world I have found this article instructive and useful. Thus far if a site wants to fix cookies on my phone or PC I try to stop further advertising coming my way. Sometimes I cant review or adjust the cookies – at which point I leave the site. My concern is that I am going in blind without adequate knowledge of any pitfalls. So a useful article – thank you.

Reply

We've helped millions of webmasters around the world find their perfect web hosting provider.

ABOUT WHOISHOSTINGTHIS.COM

In 2007, WhoIsHostingThis.com launched the world's first tool to discover which web host a website uses. Since then, we have published 1+ million words of real-user reviews, 2+ million words of content from our experts and helped millions of webmasters around the world find their perfect web hosting provider, whether it is for a personal website, blog or small business. Read more...