DELETING COOKIES IS AN EASY TASK. WHETHER IT'S NECESSARY IS ANOTHER MATTER.

Cookies aren't as evil as most stories – and some security tools – might have you believe.

A cookie is nothing more than some information a website can save on your computer that your browser then provides back to that same website the next time you return.

Seriously. That's it. That's all. That's a cookie.

It's what some sites use cookies for that has some people concerned and why you might care about things like deleting cookies, and perhaps even looking inside of them.

It works like this:

- You visit some website, e.g., amazon.com.
- That starts with your browser requesting a page at amazon.com.
- The server at amazon.com responds with the page your browser will show you *and* **some extra data**. This extra data is a 'cookie.'
- Your browser stores "amazon.com," plus the cookie on your computer somewhere, and displays the page.
- You spend some time viewing the page.
- You move on to another page on that same site, perhaps by clicking a link to "amazon.com/tech_books.html"
- Your browser requests the page "tech_books.html" from amazon.com *and sends the cookie with that request* when it asks for the page.
- The server does whatever the server does with the cookie and delivers the page to the browser to be displayed.

The important thing that makes all this work is that only cookies sent to you *by* amazon.com will be sent *to* amazon.com. This prevents one site from seeing the data that might be kept by another.

Cookies can be used for many things, but the simplest case is just remembering who you are. For your sake!

What many don't realize is every page you visit on the internet is completely stand-alone. So when you login to a site like Amazon, there's no inherent

mechanism to pass along to the next page that you visit on that site that you are in fact logged in.

The result would be that each attempt to visit a new page on Amazon would say in effect, “I don’t know you. Please login,” and you’d be faced with a never-ending series of login screens.

Simply storing something that identifies you as a user is one way that sites can keep track and not force you to login for every page. The data actually stored is rarely in a form that is obvious (for security purposes) but contains enough information for the server to know who you are, the fact that you’ve logged in, and that you’re authorized to see the next page.

How cookies track

Much has been made about tracking cookies, but there’s nothing at all *technically* different between cookies that “track” you, and cookies that keep you from having to login over and over again.

Here’s the scenario:

- You visit some website, say dailybeast.com
- That site contains advertisements provided by a large advertising network.
- The advertisements that show on dailybeast.com pages come *from* the servers at doubleclick.net (this is just an artificial example).
- That means that the doubleclick.net server can leave cookies on your machine just like any other website.

So far, you’ve visited a single site and the advertising network it uses has been allowed to leave a cookie on your machine.

Now you keep on browsing:

- You visit some other website, say somerandomservice.com (also artificial).
- Somerandomservice.com uses the same advertising network that dailybeast.com does: doubleclick.net.
- When an ad is to be displayed on somerandomservice.com, it is fetched from doubleclick.net and the request sends any cookies for doubleclick.net to the doubleclick.net server. Even though the doubleclick.net cookies were created during your visit to dailybeast.com, the cookies were in fact associated with doubleclick.net.

The advertising network now has the data to know that your computer visited both dailybeast.com *and* somerandomservice.com, and as long as the pages you saw had ads, how often you visit each, and what pages you visited while you were there.

Multiply that by all the sites you visit, all the different advertising networks that exist and you can imagine that a lot of back-end data analysis can determine really interesting patterns of people visiting assorted sites.

Third-party cookies

As stated in the above example, the doubleclick.net cookies were sent back to the server that they came from, the doubleclick.net server, even though the page you had requested was from somerandomservice.com. That's how cookies operate – at a domain or server level.

Many browsers make a distinction between cookies for the sites you actually requested (somerandomservice.com), and the sites that are subsequently referenced as part of fulfilling that request (doubleclick.net). The latter are called "third-party cookies."

You are the first party, the site you actually request is the second party, and all the other sites are so-called "third parties."

Most browsers allow you to turn off third-party cookies, meaning that the cookies created by third-party requests such as advertising networks are simply not created at all or are never sent.

They're tracking me!

No, they're not.

Yes, they are, but …

*they don't care about **you** specifically*.

Sorry, but we aren't that important or interesting to track as individuals.

The sheer volume of data alone makes tracking any one individual an incredibly difficult task.

What's much more interesting is aggregate data:

For example, data that shows that people who visit this page frequently are likely to respond to these advertisements. This type of tracking can also be used to perhaps prevent people whose online behavior appears to be similar to men from being shown advertisements designed for women.

You get the idea. They don't track at the individual level, but they use the data en masse to do things like provide more highly targeted and interesting ads or perform market research.

That's not to say that cookies can't be misused; it's just that it's typically a lot more work than it's worth.

Managing Cookies in Edge:

1. Open Edge.
2. Press the three-dot More Actions button on the top right.MORE: These Windows 10 Keyboard Shortcuts Will Save You Clicks.
3. Select Settings from the menu that shows up.
4. Tap or click View Advanced Settings. You'll need to scroll down to the bottom of the page.
5. Press the dropdown arrow under the Cookies field.
6. Select Block All Cookies or Block Only Third Party Cookies if you want to disable cookies, or Don't Block Cookies if you want to enable them.

Managing Cookies in Chrome:

1. Open Chrome.
2. Click Menu icon in upper right corner.
3. Select Settings.
4. Scroll down to Show Advanced Settings.
5. In Privacy section, click Content Settings
6. Select "Block third-party cookies.
7. Click Done.

Managing Cookies in Firefox:

1. Open Firefox.
2. Click on Menu icon.
3. Click Options button.
4. Navigate to Privacy tab.
5. Select Use custom settings for history.

6. Under Firefox will: use custom settings for history.
7. Under “Accept third-party cookies”, click Never.
8. Click Close.