What are ‘cookies’ on your computer and what should you do about them?

Active Retirees 22 Sep 2021

Learn how and why the websites you visit try to track and collect data from the browser on your device.

Ever been browsing the internet and seen a message pop up on a website that says something along the lines of “Accept Cookies” with an option to agree?

You may have wondered what on Earth these ‘cookies’ have to do with your computer. Don’t worry, you’re not alone.

In this article we’ll try to lift the lid on the virtual cookie jar so you not only understand what cookies are and why they exist, but also what you should do about them.

WHAT ARE COOKIES?

Let’s start with the basics – what is this mysterious cookie? Sometimes referred to as a web cookie or browser cookie, it is definitely not an edible baked treat. The simplest explanation of a cookie is that it’s a text file with small pieces of data (think usernames, passwords and online shopping carts) used to identify your computer when you’re using a network. The data stored in a cookie is created by the network server when you connect to the internet, and this data is given a form of ID that’s unique to you and your device. When you visit a website, the server automatically reads this ID and knows the specific information to deliver.

This means internet cookies allow web browsers (such as Google Chrome and Safari) to constantly track, personalise and save specific information about your session (the time you spend on each website). In other words, cookies let websites remember *you* specifically, as well as some of your internet activities and actions, for example website logins or previous search history and pages you’ve visited.

WHAT ARE COOKIES USED FOR?

In theory at least, cookies exist to identify specific users and improve their web browsing experience. It’s worth noting that the internet as we know it wouldn’t be the same without cookies; these files perform an integral role for streamlined web browsing by helping web developers provide more personalised, convenient website visits. Without cookies, you would always need to log in again every time you left a website or rebuild the whole shopping cart on your favourite online store just because you closed the page by mistake.

Cookies are intended to be used for:

- **Managing website sessions:** Each site recognises you and recalls your individual information and preferences, such as travel and entertainment versus sport and politics.
- **Personalising content:** Cookies enable tailored promotions and advertising within your sessions. The areas you search determine the targeted ads you receive in future.
- **Tracking items:** An e-commerce site can use cookies to monitor and record the items you have viewed, then make suggestions on other related products or services that might interest you.

You don't need to be a computer whiz to guess that cookies also provide advantages to web developers. Aside from being able to personalise website experiences, cookies help free up storage space for the website because the data is stored locally on your device rather than the server.

ARE COOKIES GOOD OR BAD?

So, what's the catch, you ask? First of all, cookies themselves are not harmful or dangerous. They will never infect your computer with a virus or malware. However, it is possible for cookies to be 'hijacked' by a cyber-attack, meaning hackers could gain access to your browsing sessions and histories. Therefore, the major downside of cookies is they can sometimes create vulnerabilities to your internet privacy which, as you probably know, is a serious and often overwhelming concern. If a cyber-criminal is spying on your information, cookies are likely involved.

Not all cookies are made equal, or shall we say equally threatening. The origin of the cookie is the key factor. For example, a 'first-party' cookie is created directly by the website you're using and is generally safe – assuming the website is reputable and hasn't been compromised. On the other hand, 'third-party' cookies can be more problematic because they are generated by different websites, not the pages you're currently browsing. These types of cookies are usually linked to ads on the page.

All that said, a basic understanding of cookies and internet security does go a long way to protecting you and your internet activity against unwanted eyes.

WHEN TO ALLOW OR REMOVE COOKIES

We've seen that carefully managed cookies can enhance your internet experience. At the same time, while removing cookies might help mitigate the risk of a privacy breach, it could also make websites harder to navigate.

Keep in mind you can control the cookies on your device by adjusting your browser settings. Choosing whether to allow or remove cookies may come down to your preference for convenience versus security risk. That's entirely up to you, but the more you know the better equipped you will be to make an informed decision that's right for you.

Regardless of your overall stance, it's prudent to periodically clear the cookies and other site data from your browser for a fresh start. Happy and safe browsing!

Active Retirees
Probus South Pacific Limited