What Are Cookies?

us.norton.com/internetsecurity-privacy-what-are-cookies.html

Mention “cookies,” and most people expect a treat to appear. When talking about computers, however, cookies aren’t what’s on the dessert menu. In fact, they’re not even physical objects. Yet they do a great deal of the work that makes it possible for you to browse the Internet—and they can cause trouble if you don’t know how to manage them.

Meet the Cookie

A computer “cookie” is more formally known as an HTTP cookie, a web cookie, an Internet cookie, or a browser cookie. The name is a shorter version of “magic cookie,” which is a term for a packet of data that a computer receives, then sends back without changing or altering it.

No matter what it’s called, a computer cookie consists of information. When you visit a website, the website sends the cookie to your computer. Your computer stores it in a file located inside your web browser. (To help you find it, this file is often called “Cookies.”)

What Do Cookies Do?

The purpose of the cookie is to help the website keep track of your visits and activity. This isn’t always a bad thing. For example, many online retailers use cookies to keep track of the items in a user’s shopping cart as they explore the site. Without cookies, your shopping cart would reset to zero every time you clicked a new link on the site. That would make it impossible to buy anything online!

A website might also use cookies to keep a record of your most recent visit or to record your login information. Many people find this useful so that they can store passwords on commonly used sites, or simply so they know what they have visited or downloaded in the past.

Different types of cookies keep track of different activities. Session cookies are used only when a person is actively navigating a website; once you leave the site, the session cookie disappears. Tracking cookies may be used to create long-term records of multiple visits to the same site. Authentication cookies track whether a user is logged in, and if so, under what name.

How to Manage Your Cookies

Under normal circumstances, cookies cannot transfer viruses or malware to your computer. Because the data in a cookie doesn’t change when it travels back and forth, it has no way to affect how your computer runs.

However, some viruses and malware may be disguised as cookies. For instance, “supercookies” can be a potential security concern, and many browsers offer a way to block them. A “zombie cookie” is a cookie that recreates itself after being deleted, making zombie cookies tough to manage. Third-party tracking cookies can also cause security concerns, since they make it easier for parties you can’t identify to watch where you are going and what you are doing online.

Here’s how to manage your cookies in order to protect your online activity from prying eyes:

- **Open your browser.** Because cookies are stored in your web browser, the first step is to open your browser. Popular browsers include Firefox, Chrome, Safari, and Internet Explorer.

- **Find the cookie storage.** Each browser stores cookies in a slightly different location. In Internet Explorer 9, for example, you can find them by clicking “Tools,” then “Internet Options,” then “Privacy.” In Chrome, choose the Chrome menu on the toolbar, then click “Privacy.” Most browsers store cookie settings under the privacy options.
- **Choose your setting.** Every browser gives you a range of options for handling cookies. Internet Explorer, for instance, has a slider that you can adjust for greater or lesser amounts of protection. Chrome both lets you delete existing cookies in a single click and choose how future cookies are collected or stored.

Banning all cookies makes some websites difficult or impossible to navigate. However, a setting that controls or limits third-party and tracking cookies can help protect your privacy while still making it possible to shop online and carry out similar activities.