

What are Internet Cookies? Are Cookies safe?

Many people are interested in cookies and why any security solution covers the cookie area to protect the device. Can they harm a computer? How are cookies and spyware connected? This article tries to shed some light on these aspects.

What are cookies on a computer?

A cookie is a tiny text file placed on your device by a website you visit.

« Cookies are small files that websites put on your PC to store info about your preferences. Cookies can improve your browsing experience by allowing sites to remember your preferences or by letting you avoid signing in each time you visit certain sites. » (Source: [Microsoft](#))

They are essentially your identification cards and cannot be executed as code or deliver viruses. They are uniquely yours and can only be read by the web server that assigned them to you. For example, a web-based email service (such as Yahoo or Hotmail) uses cookies for identification purposes (the option “Remember me on this computer”). More information on what cookies can do and how to block or allow them is available at the above-mentioned online resource.



Cookies on a computer

Within the Internet industry, cookies are described as small files containing information about individual computers that advertisers can analyze and use to track your online interests and tastes. In this realm, cookie technology is still being developed, and the intention is to target ads directly to what you've said your interests are. It's a double-edged sword for many people because, on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves “tracking” and “following” where you go and what you click. Understandably so, there is a debate over privacy, and many people feel offended by the notion that they are viewed as an “SKU number” – the bar code on the back of packages that gets scanned at the grocery check-out line. While this viewpoint may be extreme, in some cases it is accurate.

Are cookies safe?

A cookie itself cannot harm the computer, as it does not and cannot hold code. Therefore, it cannot perform an action itself. However, the cookie can support or help malicious actions to be taken on the respective system. Even more, being a plain text file, they are vulnerable, meaning that they can be “harvested” by other applications.

How do cookies affect you?

As seen, the cookies themselves cannot harm the computer. Still, they can contain certain information to lead a possible attacker to the respective computer. For example, we will consider that an attacker releases a Trojan in the wild to gain control over several computers. This Trojan’s payload contains dropping a Backdoor to open a port, changing the homepage of the browser, and placing a “malicious” cookie in the browser’s cookie area. When the unsuspecting user launches the browser, then it automatically connects to the new homepage, namely the attacker’s website. Once this is done, the malicious cookie is being read, and the attacker becomes aware of the fact that the computer is infected. By knowing this, it becomes a piece of cake to take over the computer using some exploits or the open port.

Let’s say that the user becomes aware of the infection and manages to remove the Trojan and the Backdoor from the computer. But if the cookie remains on the computer, it can supply the information again to the attacker if the user “manages” to access the untrusted web page again. The computer is therefore exposed once again to a possible attack.

So, a cookie is used to provide information about a device, but it is not responsible for the attack itself. A cookie is vulnerable though to third-party attacks.

Should I delete cookies?

If you share your device with other people, and you don’t want them to be able to auto-login to your online accounts or view your browsing history, deleting cookies is a good idea. This practice can help improve your privacy. Whether you are using a Windows computer or a Mac, you will find a few useful articles on clearing cookies at the end of this article.

Additionally, many web browsers offer Incognito mode also known as private or anonymous browsing. Incognito browsing blocks websites from placing cookies on your system. It may be a handy tool to use when checking your email from a public computer or hiding your browsing history from others who use the same device.

Does Bitdefender scan for cookies?

Bitdefender scans for cookies. It detects both viral and spyware attacks using the signature-based mechanism. This feature is included in the default configuration of the security solution, so you are not required to perform further actions after installing Bitdefender.

Moreover, with the [Bitdefender Anti-tracker](#) extension activated in your web browser, you avoid being tracked by tracking cookies. Your data remains private while you browse online, and you speed up the time websites need to load.

In conclusion, when talking about cookies, it's important to know how to protect from third-party or tracking cookies or how to protect a computer against cookie harvesting. Since cookies are necessary for browsing or the fact that the cookie traffic is invisible to the computer user, a "cookie control" module is needed to help internet users.