Welcome To All About Cookies.org

What Are Cookies In Computers?

Also known as browser cookies or tracking cookies, cookies are small, often encrypted text files, located in browser directories. They are used by web developers to help users navigate their websites efficiently and perform certain functions.

Due to their core role of enhancing/enabling usability or site processes, disabling cookies may prevent users from using certain websites.

Cookies are created when a user's browser loads a particular website. The website sends information to the browser which then creates a text file.

Every time the user goes back to the same website, the browser retrieves and sends this file to the website's server.

Computer Cookies are created not just by the website the user is browsing but also by other websites that run ads, widgets, or other elements on the page being loaded.

These cookies regulate how the ads appear or how the widgets and other elements function on the page.

For Managing cookies for different browsers see here

Standard Uses For Browser Cookies

Website servers set cookies to help authenticate the user if the user logs in to a secure area of the website. Login information is stored in a cookie so the user can enter and leave the website without having to re-enter the same authentication information over and over. More information

Session Cookies are also used by the server to store information about user page activities so users can easily pick up where they left off on the server's pages. By default, web pages really don't have any 'memory'. Cookies tell the server what pages to show the user so the user doesn't have to remember or start navigating the site all over again.

Cookies act as a sort of “bookmark” within the site. Similarly, cookies can store ordering information needed to make shopping carts work instead of forcing the user to remember all the items the user put in the shopping cart.

Persistent or tracking Cookies are also employed to store user preferences. Many websites allow the user to customize how information is presented through site layouts or themes. These changes make the site easier to navigate and/or lets user leave a part of the user's “personality” at the site.

For Information on session and persistent and tracking cookies, see here

Cookie security and privacy issues

Cookies are NOT viruses. Cookies use a plain text format. They are not compiled pieces of code so they cannot be executed nor are they self-executing. Accordingly, they cannot make copies of themselves and spread to other networks to execute and replicate again.

Since they cannot perform these functions, they fall outside the standard virus definition.

Cookies CAN be used for malicious purposes though. Since they store information about a user's browsing preferences and history, both on a specific site and browsing among several

sites, cookies can be used to act as a form of spyware.

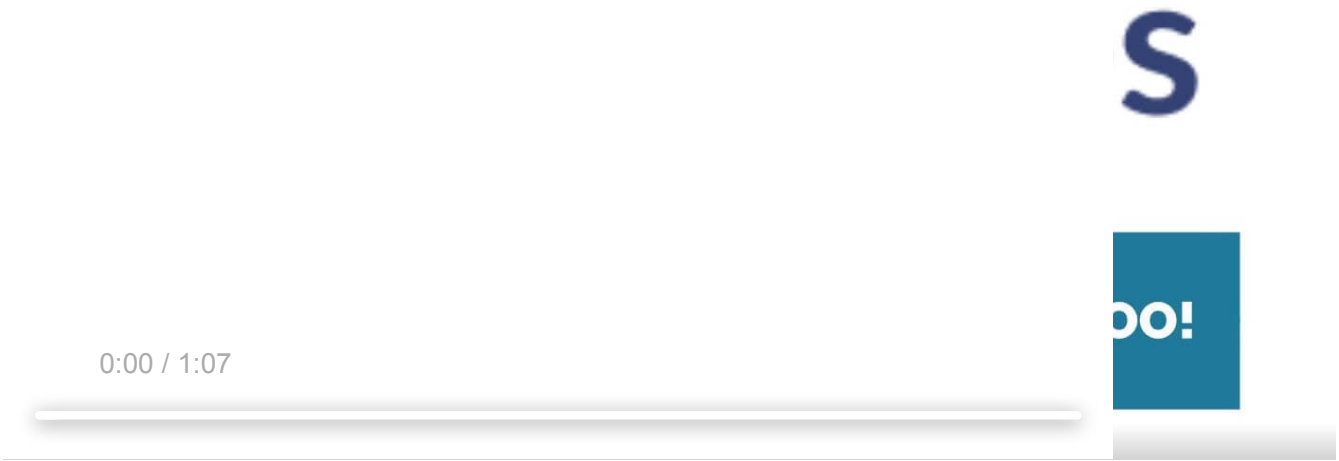
Many anti-spyware products are well aware of this problem and routinely flag cookies as candidates for deletion after standard virus and/or spyware scans.See here for some privacy issues and concerns.

The way responsible and ethical web developers deal with privacy issues caused by cookie tracking is by including **clear descriptions of how cookies are deployed on their site.**

If you are a web developer and need advice on implementation of cookies and a privacy policy, you can contact us by the enquiry form at the bottom of the page.

These privacy policies should explain what kind of information is collected and how the information is used. Organizations utilising and displaying a proper and useful cookie's policy and privacy policy include: LinkedIn Networkadvertising.org.

Most browsers have built in privacy settings that provide differing levels of cookie acceptance, expiration time, and disposal after a user has visited a particular site. Backing up your computer can give you the peace of mind that your files are safe.



Computer Cookies Help

Computer cookies make our experience on the internet easier, quicker and much less complicated.

Imagine trying to login to your favourite website or social media account or email and having to remember and type in your username and password every time, it would be almost impossible. Just to cope and make it easier you would probably start using the same username and password for every account which would be very dangerous and compromise your cyber security cookies are essential for internet surfing.

They help you and they help the website owner by helping to know their audience and customer.

Cookies help identify and recognise that it's you and allow you quick entry and they also help the website owner to identify the bad and malicious visitors who may be bots trying to enforce their way into the code of the website looking for vulnerabilities to place malicious and hijacking code that will give you malware.

Cookies don't identify you personally and they can't tell who you are but they can remember the device you are using and thus make it simpler for you to use.

Other cookie-based threats

Since identity protection is highly valued and is every internet users right , it pays to be aware of what threat cookies can pose.

As cookies are transmitted back and forth between a browser and website, if an attacker or unauthorized person gets in between the data transmission, the sensitive cookie information can be intercepted.

Although relatively rare, this can happen if the browser is connecting to the server using an unencrypted network like an non-secured WiFi channel.

Internet security is only attainable if you regualrly use a anti-virus protection programme. See our anti virus protection section.

Other cookie-based attacks involve exploiting faulty cookie-setting systems on servers. If a website doesn't require browsers to use encrypted channels only, attackers can use this vulnerability to trick browsers into sending sensitive information over insecure channels.

The attackers then siphon off the sensitive data for unauthorized access purposes.

New Laws for the use of cookies and other technologies that store online user information.

On May 26th 2011, new rules governing the use of cookies by websites comes into force in Europe.

Rather than the "Opt out" option for website visitors, websites will need to specifically gain the consent of their visitor and they must "Opt In" to be able to store cookies on their computer or other devices.

This is expected to be difficult to manage and enforcement will more than likely be done subtlely and with encouragement rather than with the threat of fines and penalties.

Businesses in the EU have some great resources that can help them with their cookie compliance. The European Union has a internet handbook that explains to businesses their requirements under the legislation and has a 'cookie kit" to help them comply.

What does the new law say?

The new requirement is essentially that cookies can only be placed on machines where the user or subscriber has given their consent.
6 (1) Subject to paragraph (4), a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.
(2) The requirements are that the subscriber or user of that terminal equipment--
(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
(b) has given his or her consent.
(3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.
“(3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends o

sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent.
(4) Paragraph (1) shall not apply to the technical storage of, or access to, information--
(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

More information on the new changes can be found here.

Key tips for safe and responsible cookie-based Web browsing

Due to their flexibility and the fact that many of the largest and most-visited websites use cookies by default, cookies are almost unavoidable. Disabling cookies will lock a user out of many of the most widely-used sites on the Internet like Youtube, Gmail, Yahoo mail, and others.

Even search settings require cookies for language settings. Here are some tips you can use to ensure worry-free cookie-based browsing:

Customize your browser's cookie settings to reflect your comfort level with cookie security or use our guide to delete cookies.

If you are very comfortable with cookies and you are the only person using your computer, you may want to set long expiration time frames for storing your personal access information and browsing history.

If you share access on your computer, you may want to set your browser to clear private browsing data every time you close your browser.

While not as secure as rejecting cookies outright, this option lets you access cookie-based websites while deleting any sensitive information after your browsing session.

Install and keep antispyware applications updated

Many spyware detection, cleanup applications, and spyware removers include attack site detection. They block your browser from accessing websites designed to exploit browser vulnerabilities or download malicious software.

Make sure your browser is updated

If you haven't already, set your browser to update automatically. This eliminates security vulnerabilities caused by outdated browsers. Many cookie-based exploits are based on exploiting older browsers' security shortcomings.

Cookies are everywhere and can't really be avoided if you wish to enjoy the biggest and best websites out there. With a clear understanding of how they operate and how they help your browsing experience, you can take the necessary security measures to ensure that you browse the Net confidently.

Managing Mobile Cookies And Security

The mobile landscape is so much broader than a single platform.

We cover mobile cookie use plus cyber security issues that can be found in the mobile sector.

Knowing how to safely surf the web is one of the most important aspects of personal cyber security and education is one of the most powerful tools.

Included below are a few points to keep in mind when using your Android/iPhone (or any mobile device) to ensure that you are safe and secure on the web.

- Cookies are just text files that store information about your computer or mobile device. These cookies can be necessary for the website to operate and function, if you would like to learn how to manage mobile cookies click here.
- Be sceptical! Always research a program or application before installation. Research the application and the app developer to establish credibility. Review the product/developer

website for customer support phone number or email and review the social media pages to see what people are saying about the product.

- Avoid downloading apps or programs that found you. If you did not actively seek a program then avoid installing apps from pushy ads or automatic downloads.
- Stay current with application and operating system updates. Updates often and include security patches that are designed to fix newly discovered vulnerabilities.
- Install and USE an antivirus application to protect you from threats that slip past your personal defence.