

What are Flash Cookies and how do they work?

[< Back to News](#)[Next article >](#)

What are flash cookies? How can you get rid of them?



Contents [hide]

- 1 Learn more about how Flash cookies work
- 2 How to control Flash cookies
- 3 What are super-cookies and flash cookies?
 - 3.1 How do I get rid of Flash cookies?
 - 3.1.1 Change your Flash preferences
 - 3.1.2 Manually delete Flash cookies This is also a good way to check that other methods have worked properly.
 - 3.2 Use a dedicated Flash cookie cleaner utility
 - 3.3 Use Google Chrome or Internet Explorer to delete Flash Cookies

A minor furor has been raised about privacy issues regarding Flash cookies. These cookies are small pieces of information stored and accessed by Adobe Flash, the browser plug-in used by sites such as from YouTube.



<https://www.cookiescan.com/what-are-flash-cookies-how-do-they-work/>

Help

1/4

Some users are going so far as to sue companies that use these innocuously named tracking tools, which most people never even knew existed.

Learn more about how Flash cookies work

If you are concerned about your privacy online, it's worth learning about how Flash cookies work and what you can do to control them.

Locally stored files are common currency for Internet browser software. Every time you surf the Internet, your browser collects bits and pieces of information from the sites you visit, either in the form of cache, which stores photos and site data on your hard drive to help speed up page loading, or cookies, which are small files deposited on your computer so websites can remember certain things about you.

(Whether you've been to their site before, added something to your shopping cart, or logged in with a username and password, for example.)

But cookies aren't just deposited by site hosts. Advertising companies, whose ads are often present across multiple sites visited by a given user, can plant cookies of their own, giving them a window into browsers' surfing habits.

This rightly makes some people uncomfortable, so browser makers have for years included tools to clear local storage and cookies, limit their use in the first place, or specifically block third-party cookies. Enter Flash cookies.

Like your browser, the Flash plug-in displays all kinds of content -animation, web apps, text, and images – and, accordingly, stands to benefit from local storage. Instead of using the browser's local storage system, though, it has its own.

Adobe tells Popular Mechanics this capability is “a required capability [for Flash] to support rich Internet applications,” and that it helps provide “a better user experience.” The problem is, some sites are using Flash local storage for an entirely different purpose.

“Clearly enough consumers have said ‘no’ to cookie-based data mining that advertisers have had to invest in new technologies to track user data,” says Ben Nell, Senior Security Engineer at Foreground Security.

He's talking, of course, about Flash.

“Flash cookies were designed to track user preferences in Flash applications, and their adoption as a mechanism to keep tabs on our browsing behavior is recent enough that tools that many consumers rely on to clear their cache of advertisers' cookies aren't even looking for them.”

In other words, the Flash plug-in is able to store data locally just like your browser does, but in a different location on your hard drive.

“And since Flash is an add-on component,” says Nell, “built-in browser controls over standard cookies don't apply to Flash cookies.”

Such is the problem with Flash local storage: You're probably not aware of it, nor are you in control of it. But that doesn't mean you can't be. By right-clicking any Flash content, you can access local storage settings for a particular Website (i.e., YouTube.com), and reduce the locally stored content to 0, deleting any data the site has previously planted on your computer and preventing future storage.

How to control Flash cookies

If you want more control over Flash cookies in general, you'll need to open up the Adobe Settings Manager, accessible either by right-clicking Flash content and clicking “Global Settings,” or by navigating directly to your storage settings through the [Flash Website](#). Here you can clear some or all of your Flash cookies manually

through the Website Storage panel, or even turn off Flash Storage completely, though the latter may prevent some sites from working properly.

The main problem here – that sites can store and maintain data and tracking cookies through your Flash plug-in, regardless of your browser's privacy settings – is something Adobe is aware of and says will soon be addressed. The latest version of Flash (10.1) already supports the private browsing features of browsers like Firefox and Internet Explorer, which prevent data from being stored locally when activated.

Additionally, Adobe says, the company is working with “major browser vendors to develop effective approaches that allow users to control local storage in Flash Player directly from their browser privacy settings”—a fix that could eliminate this problem entirely.

For now, though, the only browser that includes Flash storage settings in its native preferences panel is Google Chrome, and even there it's just a link to the aforementioned online Flash Settings panel. The only way to be sure of what sites are storing on your computer, then, is to check for yourself.

The original article can be read here – <https://www.popularmechanics.com/technology/security/how-to/a6134/what-are-flash-cookies-and-how-can-you-stop-them/>

What are super-cookies and flash cookies?

The most common kind of supercookie is a Flash cookie which uses Adobe's multimedia Flash plugin to hide cookies on your computer that cannot be accessed or controlled using your browser's privacy controls (at least traditionally, most major browsers now include deletion of Flash cookies as part of their cookie management).

Because these cookies are stored outside the browser you cannot protect yourself by using a different browser (for example one for your banking website and another for riskier web surfing), as the Flash cookies will be available to all browsers (i.e. a cookie acquired when using Chrome will also be available to websites when using Firefox). In addition to this, Flash cookies can hold up to 100kb rather than just the 4kb held by HTTP cookies.

One of the most notorious (and freaky!) kinds of Flash cookie is the 'zombie cookie', a piece of Flash code that will regenerate normal HTTP cookies whenever they are deleted from a browser's cookie folder.

How do I get rid of Flash cookies?

Change your Flash preferences

This is always worth doing, although some LSOs seem adept at evading the preferences settings.

1. To remove existing site cookies go to the [Adobe Website Storage Settings Panel](#), where you will see a list of Flash cookies on your computer. If you recognize any of the websites in the list and visit them regularly, then you may want to keep their cookies as they can provide useful functionality, but you can delete the others.
2. To prevent new sites from writing cookies, go to the [Adobe Global Storage Settings Panel](#) (or just click on the Global Storage Settings tab in the Settings Manager), drag the slider to 'None', and click 'Never Ask Again'. Note that doing this may create problems with websites that rely on Flash functionality.

Manually delete Flash cookies This is also a good way to check that other methods have worked properly.

In Windows open an Explorer window and type '%appdata%' into the search bar. Double-click Macromedia -> Flash Player -> macromedia.com -> support -> flashplayer -> sys (we told you they were hidden away!). Any folders you see (which should contain a .sol file, which is the actual cookie) can be deleted.

In OSX try going to Users -> username -> Library -> Preferences -> Macromedia -> Flash Player-> and look for any .sol files in the folders

In Linux go to home -> username/ .macromedia -> Flash_Player -> macromedia.com -> support -> flashplayer -> sys, or run the command 'find ~/.macromedia/ -type f -name settings.sol -exec rm -v {} \;'

Use a dedicated Flash cookie cleaner utility

Examples include [GrekSoft Flash Cookie Remover](#) (Windows) and [FlushFlash](#) (Windows and OSX).

Use Google Chrome or Internet Explorer to delete Flash Cookies

Modern versions of Chrome, Internet Explorer (IE8+), and Firefox work with Flash Player 10.3+ to delete Flash cookies automatically, using the browsers' built-in Clear History functions. While we applaud this move, which uses the [NPAPI ClearSiteData](#) API, it is not perfectly implemented and we found LSOs on our system after using it.

[◀ Back to News](#)[Next article ▶](#)

Ensure your website is PECR and ePrivacy compliant

Create a FREE CookieScan account today and start managing your cookie consent.

[Get Started](#)

[Privacy Policy](#) [Terms Of Use](#) [Sitemap](#) [Status](#)

© CookieScan 2024. All rights reserved.