**What are cookies and supercookies? How do you remove them?**

As many computer users already know, most websites will download what are known as “cookies” onto your computer after you visit the site. Quite often, these browser-based files usually carry fairly basic information that makes web browsing much easier and faster with consecutive site visits. Most cookies are fairly harmless and indeed do help to make your browsing experience more enjoyable by storing information that reduces the loading times on for different pages, among other tasks.

For example, if you visit a website like Amazon to do some online shopping, you may log in, load your digital cart full of items, but then decide not to buy anything until later in the day. You might be surprised and somewhat relieved when you come back to Amazon to find that you’re still logged into the site and all of the items still in your cart. The persistent login and stored cart items are recorded onto a cookie file that Amazon (or any other site) quickly reads as you head back to the site. This process ultimately improves your browsing and online shopping experience.

Some cookies will automatically be deleted after your website session is over (known as session cookies). Others, known as persistent cookies, may be removed after a few days or may be coded to automatically delete after a [few thousand years](https://www.google.com/search?q=how+often+do+cookies+expire&oq=how+often+do+cookies+expire&aqs=chrome..69i57j0.10023j0j7&sourceid=chrome&ie=UTF-8). In general, if you want to delete most cookies, there are three easy ways to do so:

* **Go to your browser settings and use the tool that removes cookies (usually located with the browser history and cache deletion option)**
* **Use an antivirus tool to remove malicious cookies, including tracking cookies**
* **Manually locate the cookies on your computer and delete them one by one, or en masse (expert-level and not recommended for most users, as this could result in accidental deletion of critical or desired files)**

For regular cookies, the first two options will work perfectly. All normal cookies and even malicious and tracking cookies are stored on your computer somewhere. All you need to do is use the tools at your disposal to delete them.

**Supercookies are different — and harder to delete**

There are two types of files currently identified as “supercookies”. One is also known by two other names: “Flash cookie” or “Local Shared Objects” or LSOs. Flash cookies, which are often located in online video advertisements, store information in a similar way to browser-based HTTP cookies, with the exception that the information is primarily related to the Flash objects. Information on Flash cookies can also be useful, such as recording where a video was stopped to make it easier to load the same place, or storing saved information for a Flash-based browser game.

Flash cookies and may also be saved in different locations on a user’s hard drive (hence the name “Local Shared Objects”). As a result, normal cookie removal steps may not delete them, leaving any malicious Flash cookies on your machine and capable of collecting and report data without your knowledge or consent.

The more insidious and more difficult to remove the version of supercookies come from internet service providers (ISPs). Unlike HTTP cookies or even Flash cookies, supercookies from ISPs are associated with the devices you use to connect to the web with a tracking file created by the ISP. Those supercookies house your device’s browsing information, are stored on the ISP’s servers and contain Unique Identifier Headers (UIDH) that help the ISP recognize each device and what each device is doing online.

As you browse the web or use your device over the network, the ISP inserts information onto the data packets that let it track your activity without ever having to install anything onto your computer. You can’t delete ISP UIDH supercookies using your web browser’s cookie deletion tool, nor can an antivirus tool find and root out those supercookies files. Simply put, with no file saved on your computer to delete, you’re left with very few options to stop any ISP intent on tracking, recording, and selling data on your online activities.

For both UIDH and Flash-based supercookies, however, there are some removal options you can employ.

**How do delete supercookies**

Flash-based supercookies and ISP-based supercookies must be handled differently. We’ll start with Flash supercookies, as these do exist on your computer and can more easily be removed.

**Stop and remove Flash supercookies**

The good news here is that Adobe (the maker of Flash software) has a working solution to stop and remove Flash supercookies that can be easily done from your web browser. Flash usually has its own Settings Manager in each web browser, and you can use it to control how Flash cookies are stored along with other things.

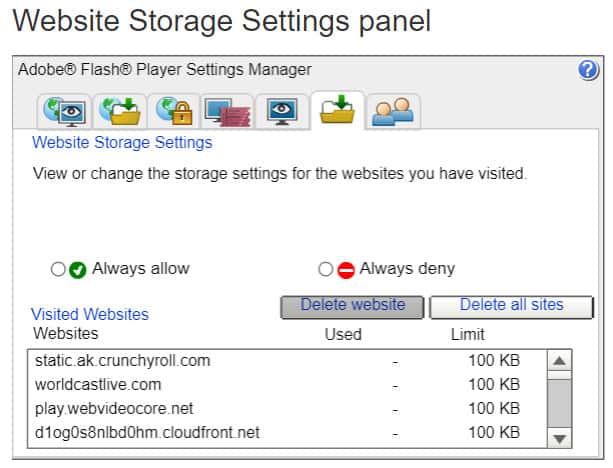
* [**Click this link**](http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager02.html)**to go to the Flash Settings Manager page**
* **If necessary, click to allow Flash Player to run on your browser\***

**\*Note:** If clicking to allow Flash Player to run in your browser doesn’t work in Chrome, you may have to change your browser settings to allow Flash. The “Ask First” setting in Chrome for Flash media may cause it not to load the Flash window properly. Try the following steps in Chrome:

* Open the page
* Click the padlock symbol on the left side the URL bar
* Click Site Settings
* **Next to Flash, click the dropdown menu and set to Allow**
* Refresh the page

In **Firefox**, you may get a dropdown menu when you click to allow Flash in the browser that asks you to allow it on the page. Make sure to click “Allow”. The page will automatically refresh to load the Flash window.

What you should be seeing is something like this:

[](https://cdn.comparitech.com/wp-content/uploads/2019/04/supercookies1.jpg)

When you open the Manager, you’ll notice a few different tabs. First, we’ll visit the local storage settings tab, which is the one with a yellow folder and a green arrow, but without a globe image (that’s the Global Settings Panel, which we’ll discuss in just a bit).

Here you can see which cookies have been written to your computer along with the ability to DELETE all of them. That’s something we strongly recommend. Remember, however, that there are some benefits to these cookies. If you frequent sites that use this technology (and many do) you will be deleting some of your settings with those sites and you may have to re-enter text each time you visit.

Even if you decide to push the “Delete all sites” button, you still have some work left.

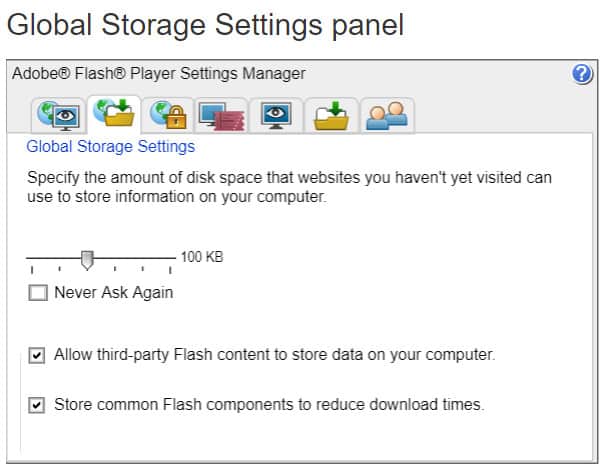
**Stopping new sites from writing cookies**

Even if you deleted the cookies that have already been written to your computer, you may want to keep new cookies from being written as well. Luckily, Adobe has created a way to do that:

Adobe Global Storage Settings Panel (accessed from the same panel as the other local removal settings).

**Next, click on the folder tab that has a globe image in the background.**

If everything goes according to plan, you should see something that looks like this:

[](https://cdn.comparitech.com/wp-content/uploads/2019/04/supercookies2.jpg)

Here you can tell Flash not to store any cookies in the future. Just drag the slider all the way to the left (“None”), and then select “Never Ask Again”. You may also want to deselect both “Allow third-party Flash content to store data on your computer” and “Store common Flash components to reduce download times”, just in case. All of those steps should prevent websites from storing Flash cookies on your computer and prevent them from utilizing Flash as a workaround for traditional HTTP cookies.

**Additional Flash supercookie removal tools**

Here are some other tools if you want 3rd party help with managing or controlling Flash supercookies:

**Windows:**

* [CCleaner](http://www.ccleaner.com/)
* [Click&Clean for Chrome](https://chrome.google.com/webstore/detail/clickclean/ghgabhipcejejjmhhchfonmamedcbeod?hl=en)
* [Better Privacy extension for Firefox](https://addons.mozilla.org/en-US/firefox/addon/6623)

**Mac OS**

* [CCleaner for Mac](https://www.ccleaner.com/download)

**Flash Cookie Storage Locations**

You can always go to the directory where the cookies are stored and remove them manually. It’s not a permanent solution – new cookies will get created in the future – but it works.

**Windows**

LSO files are stored typically with a “.SOL” extension, within each user’s Application Data directory, under Macromedia\FlashPlayer\#SharedObjects.

**Mac OS**

**For websites, Flash cookies are located in:**

~/Library/Preferences/Macromedia/FlashPlayer.

**For AIR Applications, look in:**

~/Library/Preferences/[package name (ID)of your app] and ~/Library/Preferences/Macromedia/FlashPlayer/macromedia.com/Support/flashplayer/sys

**GNU-Linux:**

LSO files are stored in ~/.macromedia.

**Stop and remove UIDH supercookies**

Simply put, there is no way to remove an ISP’s UIDH supercookies. To do so, you’d have to somehow gain access to the ISP’s servers and delete your devices’ unique data from there. Given the legal impossibility of that, your best option is to prevent ISPs from properly tracking your devices’ activity.

Note, however, that most methods to stop tracking won’t work. Your browser’s “Do Not Track” option won’t stop UIDH supercookies. And going into Incognito or other private browsing modes won’t work, as the ISP is not tracking each browser or site, but putting data identifiers based on what device you’re using and tracking *all* data exchanges wholesale.

The only way to stop ISP supercookies is to use a connection anonymization tool. The most common and easiest tool for this is a virtual private network or VPN.

**What are VPNs?**

VPNs are software you install on your computer, or as a browser plugin. VPNs will create a private data tunnel between your computer and a secure server. You’ll then access the internet from that secure server, which could be located anywhere in the world.

The only information your ISP can see is your connection to the remote server. It cannot see, and therefore cannot track, any other activity outside of that thanks to the encryption methods used by many modern VPNs. You will be able to freely browse the internet without your ISP knowing what you’re doing.

**Which VPN should I use?**

VPNs vary, however. Some maintain strict privacy standards that guarantee user privacy and anonymity. Others, however, may track their users and sell that data. Generally speaking, you’re more likely to find a trustworthy VPN if you use a paid service, as free VPNs tend to monetize their service through somewhat invasive advertisements and by collecting and selling user data.

Some of the industry-leading and most-recommended VPNs include ExpressVPN, NordVPN, IPVanish, and Cyberghost. There are more, however, so it’s important to do your research before settling on a VPN you believe will best serve your privacy needs and budget.

**For Verizon customers**

Following a court case against their use of UIDH tracking, Verizon allows customers to [opt-out](https://www.verizonwireless.com/support/unique-identifier-header-faqs/) of this type of tracking.

[**You can do so by logging into your Verizon Wireless account here**](https://www.verizonwireless.com/myprivacy/)**.**

Note that this only applies to Verizon customers, as Verizon was forced to take this move [thanks to the lawsuit](https://www.forbes.com/sites/abigailtracy/2016/03/07/verizon-wireless-fined-1-35-million-settlement-fcc-supercookies-uidh/).

To note, AT&T [claims it stopped](https://www.foxnews.com/tech/stop-carriers-from-tracking-your-mobile-browsing) using UIDH trackers. It’s quite possible other ISPs have also stopped the practice, but internet users can’t know for certain whether their ISP utilizes this type of tracking due to how it works.