What are Supercookies, Zombie Cookies and Evercookies and are they harmful?

These cookies are famous for causing lots of difficulties for those who want to remove them.

Being followed is always one of the biggest privacy issues for cookie users, but that has changed with the Internet.Although the usual cookie browser is quite useful and easy to clean up, there are other variations built to stick and track the user's browsing activities.Two of these variations are supercookies and zombie cookies (commonly known as "Evercookies").These two variants are famous because they cause a lot of difficulties for those who want to remove them.Fortunately, they have 'received' the proper attention of security researchers, and web browsers today are constantly evolving to counter these sophisticated sneaky tracking techniques.

Supercookies

The term may be a bit confusing because it is used at the same time to describe a number of different technologies, while only a few of them are actually cookies.In general, this term refers to things that can change your browsing profile to provide you with a unique ID.In this way, they support the same functions as cookies, allowing websites and advertisers to track you, but unlike cookies, they cannot be deleted.

You will often hear the term 'supercookie' used in reference to the Unique Identifier Headers (UIDH) and a vulnerability in HTTP Strict Transport Security (HSTS), although the root phrase refers to cookies originating from Top-level domain names.This means that cookies can be set for domains such as '.com' or '.co.uk', allowing any site with that domain suffix to see it.

If Google.com sets up a supercookie, that cookie will be visible to any other ".com" site.This is obviously a privacy issue, but because it is a common cookie on the other hand, most modern browsers block them by

default.Because no one talks more about this supercookie type, you will often hear more about the other two types (Zombie Cookies and Evercookies).

Unique Identifier Header (UIDH)

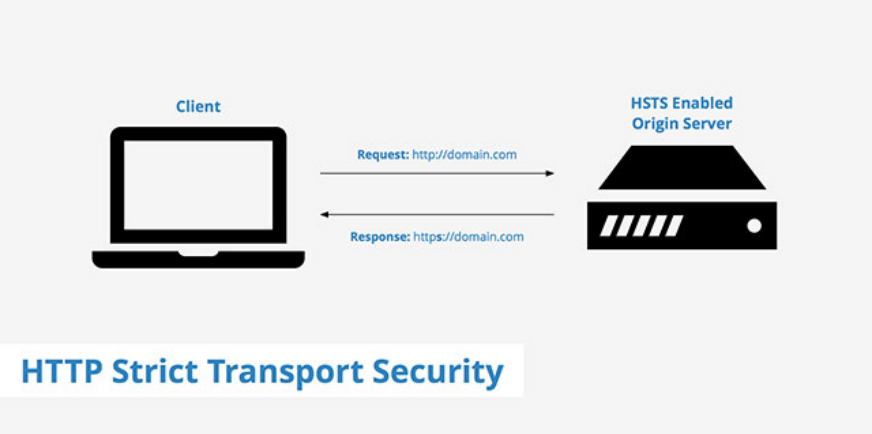
A Unique Identifier Header is usually not available on your computer, it appears between your ISP and the site's server.Here's how UIDH is created:

1. You send a request to a website to your ISP.
2. Before your ISP forwards the request to the server, it will add a unique identifier string to the title of your request.
3. This unique identifier allows sites to identify you as the same user whenever you visit, even if you have deleted their cookies.When websites know who you are, they just need to set the same cookie straight to your browser.

Simply put, if the ISP is using UIDH, it will send your personal 'signature' to every website you visit.This is mainly useful in optimizing ad revenue, but it is enough to cause discomfort to the FCC that fined Verizon 1.35 million for not informing their customers about it, or not providing Give them the option of not participating.

Apart from Verizon, there is not much data in which companies are using UIDH-style information, but consumer backlash has made it an unpopular and popular strategy.It even works only on unencrypted HTTP connections.Also, since most websites now use HTTPS by default and you can easily download utilities like HTTPS Everywhere, this supercookie is no longer a big deal and may not be possible. widely used.If you want to increase protection, use VPN.VPN ensures that your request will be forwarded to the website without attaching UIDH.

HTTPS Strict Transfer Security (HSTS)



HSTS (HTTP Strict Transport Security) is a security policy necessary to protect secure HTTPS websites against low-level attacks.The HSTS ensures that all connections to a website must be encrypted using HTTPS protocol, and never use the HTTP protocol.Currently Google is applying HSTS to 45 most advanced domain names, including domain names ending in .google, .how and .soy.

HSTS is really a good solution.It allows your browser to safely redirect to the HTTPS version of the site instead of the insecure HTTP version.Unfortunately, it can also be used to create a supercookie with the following formula:

1. Create multiple subdomains (like 'domain.com,' 'subdomain2.domain.com' .).
2. Assign each visitor to your main page a random number.
3. Forcing users to load all of your subdomains by adding them to hidden pixels on a page or redirecting users to each subdomain while loading the page.
4. For some subdomains, they require the user's browser to use HSTS to switch to the security version.For others, they leave the domain name in an unsafe HTTP form.
5. If the subdomain HSTS policy is enabled, it is counted as '1.'If it is off, it is counted as '0'.Using this strategy, the website can record a user's random ID number in binary form in the browser's HSTS settings.
6. Every time a visitor returns, the site will check HSTS policies on the user's browser, HSTS will return the original binary number to help identify the user.

It sounds complicated, but in short, the website can make your browser create and remember the security settings for multiple pages and the next time you visit, it can tell who you are through the data. get.

Apple has also come up with solutions to this problem, for example, allowing only HSTS settings to be set for one or two main domains on each site and limiting the number of redirects that sites are allowed to use. .Other browsers also have the ability to follow these security measures (Firefox's incognito mode is an example), but since there are no validations made about effectiveness, this is not Top priority for most browsers.You can solve the problems yourself by learning more about some ways to install and delete HSTS policies manually.

Zombie cookies / Evercookies

Zombie cookies, also known as Evercookie are essentially a JavaScript API created to illustrate the difficulties you will face in an attempt to delete a cookie.

Zombie cookies cannot be deleted because they are hidden outside your regular cookie memory.Local storage memory is a major goal of Zombie cookies (Adobe Flash and Microsoft Silverlight use this a lot) and some HTML5 storage can also be a problem.Zombie cookies can even be in your browsing history or in the RGB color code that your browser allows to cache.

However, many security holes are gradually disappearing.Flash and Silverlight are not an important part of modern web design and many current browsers are not vulnerable to Evercookie anymore.Because there are so many different ways that these cookies can jostle and 'parasitize' your system, there is no way to protect yourself, but the browser cleanup routine is never one. bad measure.

Are we safe?

Developing online tracking technology is a non-stop race in the security world today, so if privacy is something you particularly care about, you should probably get used to the fact that we Never be 100% secure in an online environment.

However, you do not need to worry too much about supercookies because they do not appear too popular and are increasingly prevented more aggressively.These cookies are still active until all holes are patched, and they can always be updated with new techniques.

See more:

1. How to delete cookies on Chrome with each website
2. Cookies do not damage your computer?
3. How to delete cache and cookies on Chrome, Firefox and Coc Coc
4. Instructions for deleting cookies in Windows PC

You finished reading the article "**What are Supercookies, Zombie Cookies and Evercookies and are they harmful?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.