Session Cookie Hijacking

Session cookies are temporary cookies that keep you authenticated after logging into a website that uses your credentials. They can be copied by malware on your computer that when combined with stolen credentials can give someone complete access to any data that you allow to sync across devices, such as passwords and payment methods and the ability to hijack your account. This has been found to be a big problem for Google. It is recommended for now to either turn off sync or adjust the Sync and Google Services in Chrome Settings to at least turn off sync for Passwords and Payment methods. Mobile devices have sync settings also. I found my Samsung settings under Autofill with Google - Preferences. Future data can be prevented from being stored in Google cloud servers, but previously synchronized data would have to be manually deleted. You can go to chrome.google.com/sync and click on Clear Data to remove all synchronized data from your Google account.

Google has an experimental fix called “device bound session credentials” that can be enabled in chrome://flags that ties the session cookies to the TPM security of your device. Eventually this should be a feature included in a Chrome update if it works as intended without issues. Other browsers that are Chromium based have the same vulnerability.

Extracted From Reddit Email by

r/GMail
•
3mo ago
PaddyLandau

Session (cookie) hijacking: A simple protection measure if you use a Chromium based browser

The problem

Far too many people have had their Google account stolen through session hijacking (a.k.a. cookie hijacking). This is a particularly nefarious hack, because the hacker gets immediate full access to your account on their own computer. Within seconds, you're kicked out of your own account, and it's horribly difficult to kick the hacker out and undo the damage.

A proposed solution

Since April 2025, Chromium and therefore all Chromium-based browsers have had a new protection against this type of hack. It works by tying your cookies to your physical device. Thus, copying the cookies to a different computer (as session hijacking does) will fail to allow the hacker access. This is intended to work not only with Google accounts but with any account.

Caveats:

Your computer needs TPM 2 in the hardware (most modern devices have this).
This only works with websites that support this feature.
It's still in the experimental stages.

If you already have session-hijacking malware on your computer, this might not work (it depends on the malware).

This protection is not a guarantee, but it's a good idea nevertheless. This appears to be implemented on desktops and laptops, but not (as far as I know) on any of the small devices (Android, iOS, etc.).

Chromium-based browsers include (but aren't limited to):
Brave
Chromium
Google Chrome
Microsoft Edge
Opera
Vivaldi

This feature is operating-system agnostic, so it works with Linux, MacOS, Windows, etc.
I haven't been able to test this on a Chromebook (please let me know the results if you can).
Firefox isn't Chromium-based, nor does it have this feature. Let's hope that Mozilla implements it soon.

How to turn on this protection

Step 1

In your Chromium-based browser, go to the browser's flags. How do you do this? You enter a certain URL in the
URL bar. I've tested the following four browsers:

1. Chromium: chrome://flags
2. Google Chrome: chrome://flags
3. Microsoft Edge: edge://flags
4. Opera: opera://flags

If you use a different browser, you'll have to find out what works in yours.
Enter the relevant URL in your URL bar and press Enter to get to the flags page.
The flags page (chrome://flags) on Google Chrome

Step 2

Once you have the flags page in front of you, you have to enable "Device Bound Session Credentials". The list of flags is huge and is in no obvious order, so the easiest way to find the flag is to use the search at the top of the page. Start typing "device bound session credentials". As soon as you see it, you can stop typing. Go to the flag, which should be set to "Default". Press the down-arrow to see different options. In Chrome and Chromium, I recommend choosing "Enabled with multi-session". For the other browsers, I don't quite understand the various options; the safe option is simply "Enabled", but you can look up what the other options mean for your browser. Once you've made the change, the browser will prompt you to "Relaunch". The option won't be activated until you do this.

Pass the word around! Let's give the session-hijacking hackers a hard time