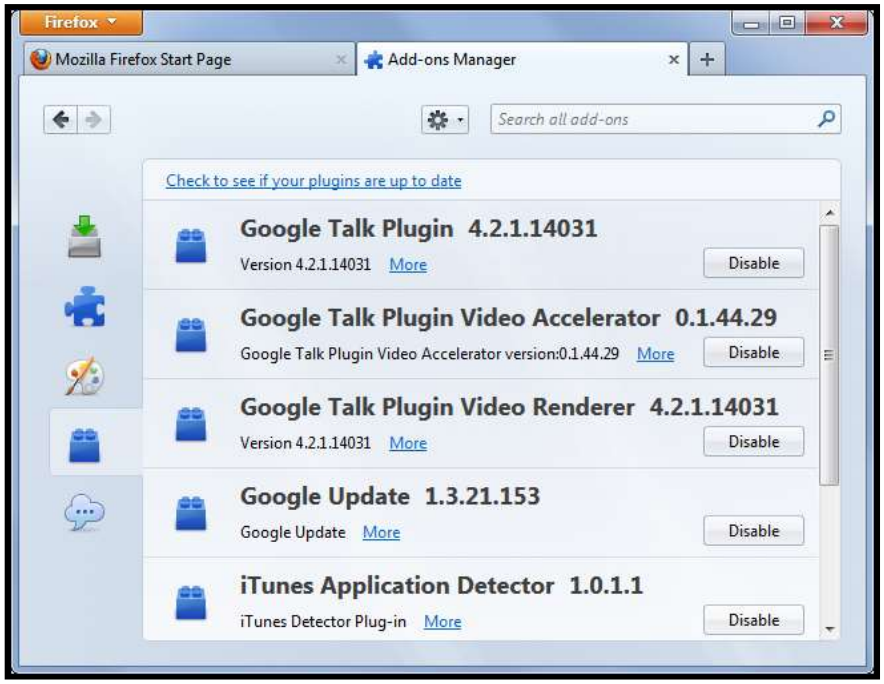
Are Bogus Browser Extensions Bumming You Out, Bubala?



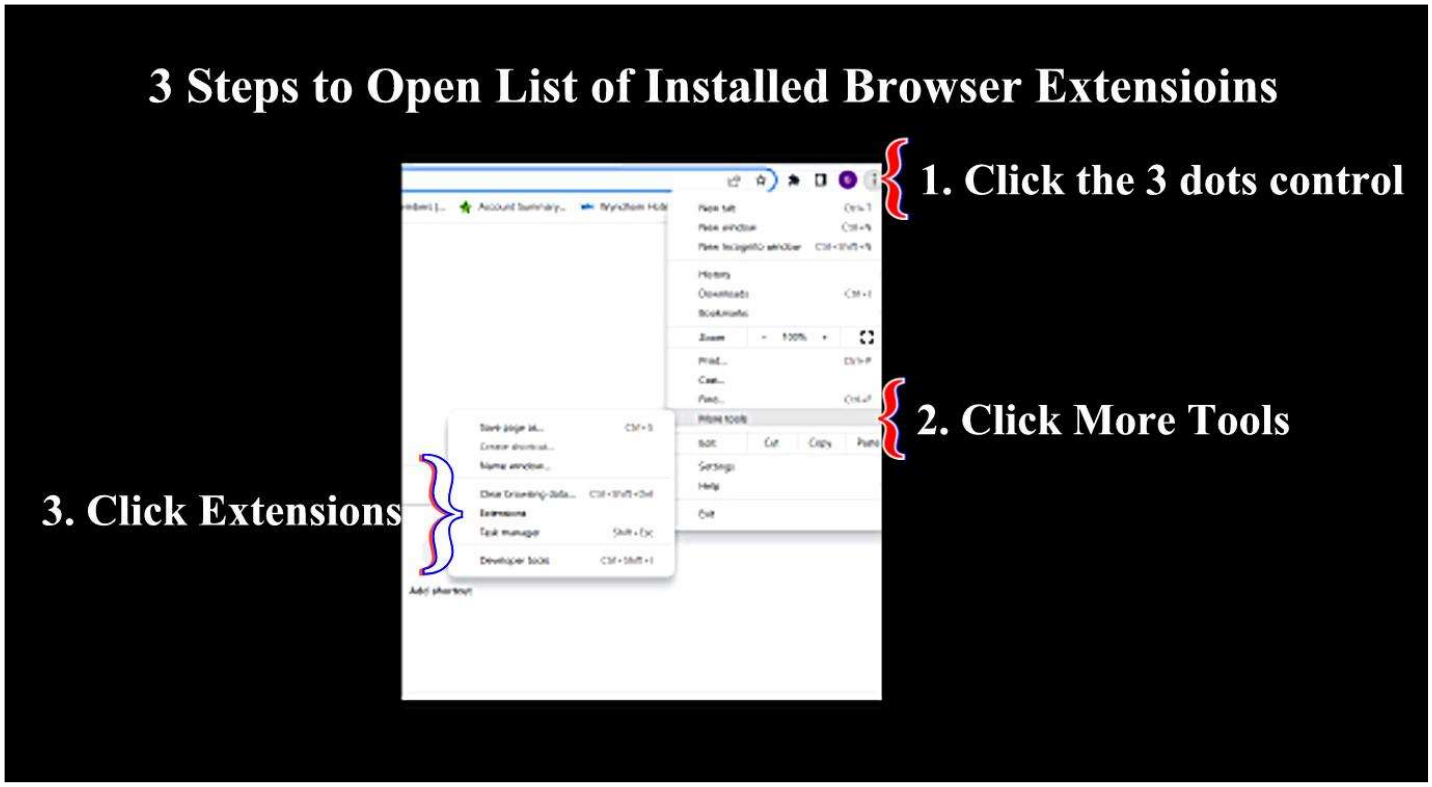
source: https://www.howtogeek.com/wp-content/uploads/2013/07/firefox-plug-ins-list.png?trim=1,1&bg-color=000&pad=1,1

This week's cybernews began with reports about rogue Google browser extensions. The rogue extension "**is masquerading as a Google Translate add-on as part of an adware campaign targeting Russian users of Google Chrome, Opera, and Mozilla Firefox browsers**," reported **The Hacker News, July 8, 2022**. Unlike many browser extension, legitimate or otherwise, this browser bad boy "**is delivered through different Windows executables that install the add-on on the victim's web browser.**" The usual method of delivery of browser extensions is the vendor's "store."

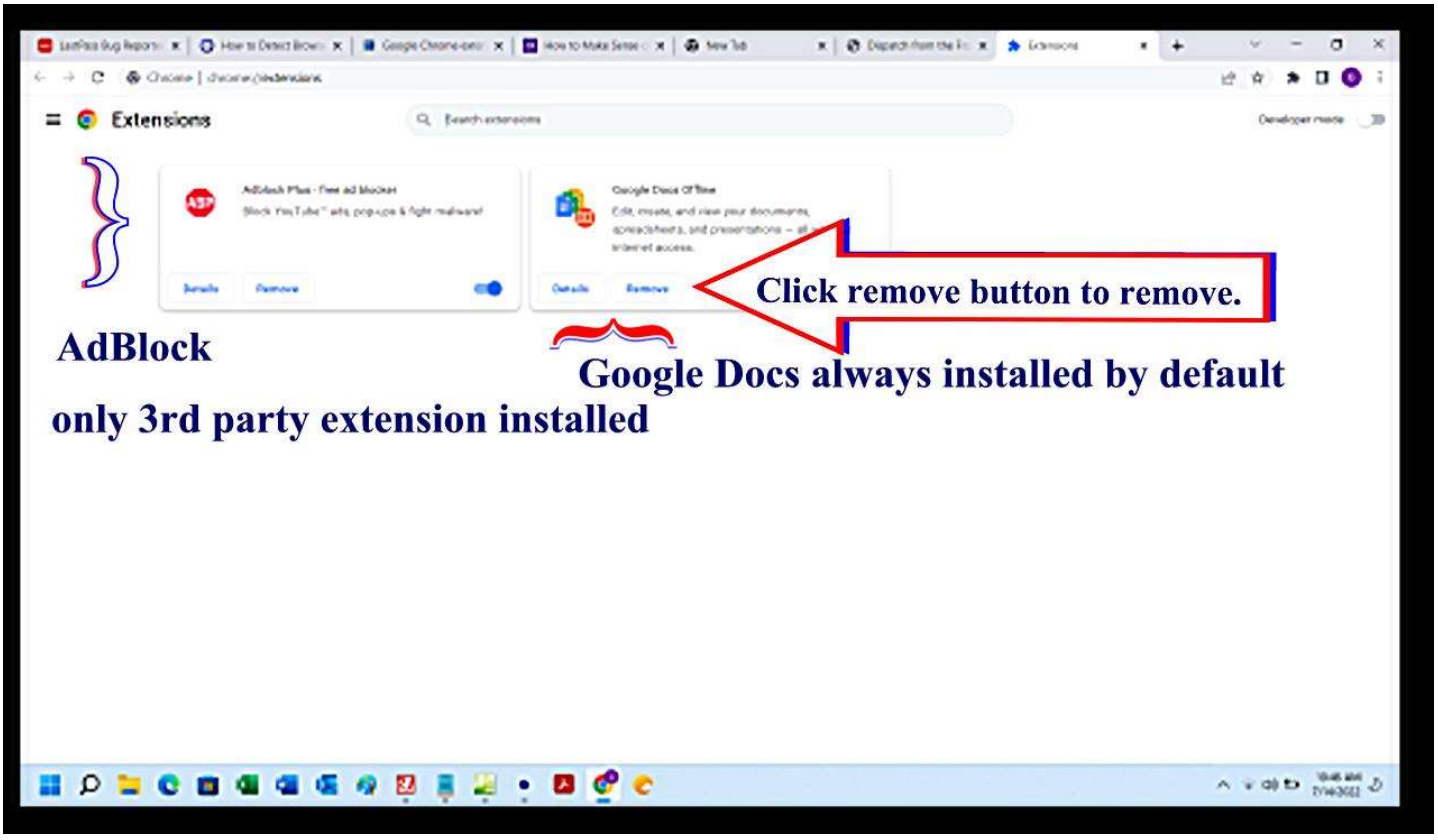
In June 2022, **BleepingComputer reported** that a developer created a Proof of Concept website that demonstrated certain Google browser extensions could be modified to track users' activities and computer processes used. **This is activity is known as fingerprinting**. That browser extensions can be used for surreptitious fingerprinting of visitors to a website as been known for some time. In 2019, LastPass fixed a browser bug "**that exposes credentials entered on a previously visited site.** " **LastPass Press Release of September 13, 2019** definitely blamed the problem on weak browser extension security.

> **Our team recently investigated and resolved a bug affecting certain LastPass extensions. Tavis Ormandy, a security researcher from Google's Project Zero, responsibly disclosed the issue to us. His report revealed a limited set of circumstances on specific browser extensions that could potentially allow an attacker to create a clickjacking scenario.**

So browser extensions are the kinds of things you certainly want to take control of. Herein we will look at Google Chrome Extensions tool because that is what most of my clients regularly use; but other browsers act similarly.



Once you have opened the browser extensions tool, you can see exactly what browser extensions are installed.



If in this list, there are browser extensions you do not recognize, simply click the **remove button**.

Now, obviously I am not big on browser extensions. One should not infer, however, that ALL browser extensions are harmful. We have already mentioned the LastPass Password Manager relies on a browser extension to work. You might have a shopping extensions that finds you discounts and coupon codes. There are various screen capture extensions, as well. In February 2022, Techrader published a list of "**The best Google Chrome extensions in 2022: do more with your browser**." Top of the list was LastPass. And I must note that **LastPass began 2022 with the announcement that the LastPass users' Master Password list had been hacked and those passwords were exposed**.

Knowing that forewarned is forearmed.
Abraham Tucker, The Light of Nature Pursued, 1768.

Back to Top

Gerald Reiff

Back to Top

next post ⟶