Read this before installing extensions to your web browser

22 July 2019, by Jefferson Graham, Usa Today

Credit: CC0 Public Domain

When Amazon offered recently to pay Prime members $10 to download its Assistant browser extension, Jeremy Tillman, who runs the ad-blocking software Ghostery, took notice. He likened it to that sweetheart deal when the Dutch bought Manhattan island for $24.

A consumer chump deal, enabling Amazon to "watch everything you do on your browser, from your online shopping habits, to your social media activity," in exchange for that $10 discount.

The Prime Day offer was for two days only and has since come and gone. But it helped put the spotlight on browser extensions, software that can add shortcuts for those of us on desktop and laptop computers.

The pros and cons of browser extensions

There are good uses for such extensions tools, which you might employ to quickly translate text, make screen captures, block ads, remember passwords and shorten URLs.

But they can also snoop on you and "eat at your processing power, take memory away," and more, says David Temkin, the chief product officer for the Brave browser.

Tillman notes that only a small percentage of browser extensions are actually bad. But "as with most things in life, there will always be bad actors looking to circumvent rules and ethical best practices to deceive and manipulate its users to make a buck."

On Apple's Safari support page, the company says extensions "add functionality" to ..."explore the web the way you want. Extensions can show helpful information about a webpage, display news headlines, help you use your favorite services, change the appearance of webpages, and much more."

For its part, Amazon's Assistant is pitched as providing shortcuts for delivery notices, and comparison shopping. What is not immediately obvious is that Amazon's browser extension watches how you shop when you visit other websites.

Rakuten concedes that its eBates shopping assistant browser extension, for instance, uses location-identifying technologies while it tries to find you good deals. The company says it "may rent, sell, and share other information that cannot be used to identify you with merchant partners, third parties, or affiliates," to monitor our usage and activity.

BeFrugal, another shopping site, says it gathers "information about your activities on this site and other sites to provide you with advertising based on

your browsing activities and interests."

In other words, you'll get even more personalized ads thrown at you based on your shopping history.

What you should do before downloading an extension

Tillman recommends always reading the privacy policies before downloading extensions, "particularly the sections related to data collection, to see if these tools are collecting and sharing data with so called 'third-party partners,' which is a strong indication that they may be selling personal data."

Temkin credits BeFrugal and Rakuten for at least actually stating what their privacy policy is. Many others don't bother with it.

His tip: Be careful before downloading an extension.

Before you download, "read the reviews, see how many times they've been downloaded," and read the privacy policy, if it's available, says Temkin. "Apply a general rule of caution because they can do a lot to your browser that you don't anticipate."

Kurt Opsahl, the deputy executive director of the Electronic Frontier Foundation, says to make sure "the permission granted to the extension makes sense for what it's designed to do."

Additionally, be sure to only download extensions from the authorized web stores-Google for Chrome, Apple for Safari and Microsoft for Edge all have them—and to steer clear of third-party extensions.

Even at that, don't download too many extensions. "Not only do they affect computer performance, but they are also a potential attack vector, so narrow their number to just a few of the most useful," advises security firm Kaspersky.

Researchers at North Carolina State University did a survey of extensions and found many were not just privacy hogs, but that they also were capable of "potentially leaking privacy-sensitive information. The top 10 most popular Chrome extensions that we confirmed to be leaking privacy-sensitive information have more than 60 million users combined," the authors Quan Chen and Alexandros Kapravelos said.

"Our results emphasize the threat browser extensions pose to user privacy, and the need for countermeasures to safeguard against misbehaving extensions that abuse their privileges," they added.

For the Amazon extension, it's not just "harmless background activity occurring as you browse—you really are giving corporations a direct look into all of your preferences, habits and vulnerabilities," says Tillman. "And in this case, for just $10." ___

APA citation: Read this before installing extensions to your web browser (2019, July 22) retrieved 1 July 2022 from https://techxplore.com/news/2019-07-extensions-web-browser.html