When Helpful Browser Add-Ons Go Rogue

Before we dive in, let's clear up one thing. A browser extension is a small add-on you install in your web browser (like Chrome, Edge, or Firefox) to add extra features. Ad blockers, coupon finders, password managers, screenshot tools, and video downloaders are all browser extensions. Because they live *inside* your browser, they can see and interact with the websites you visit, which is useful... until it's not.

Recently, security researchers discovered that over 840,000 users had installed malicious browser extensions that looked helpful but were quietly doing things they shouldn't. These extensions were available in official browser stores and used innocent-sounding names. Behind the scenes, they tracked browsing activity, redirected shopping links, and sent data to third parties. Think of it as installing a helpful assistant who secretly takes notes on everything you do.
Some of the extensions identified in this campaign include:

- Ads Block Ultimate
- Google Translate in Right Click
- Floating Player – PiP Mode
- Instagram Downloader
- Free VPN Forever
- Full Page Screenshot
- Amazon Price History
- Weather Best Forecast
- YouTube Download
-

If any of these sound familiar, it's a good idea to remove them immediately. Even if they seem to work fine, malicious extensions don't always cause obvious problems.
The good news is that protecting yourself is simple. Review your installed browser extensions regularly and remove anything you don't recognize or no longer use. Keep your browser up to date and limit extensions to only the ones you truly need. Fewer extensions mean fewer opportunities for something shady to slip in and your browser will probably run faster, too.

How to Check Your Browser Extensions

Take two minutes and do a quick extension check using the steps below.

Google Chrome

1. Click the three dots (top right)
2. Select **More tools**
3. Click **Extensions**
4. Review the list and remove anything you don't recognize or no longer use

Microsoft Edge

1. Click the three dots (top right)
2. Select **Extensions**
3. Review installed extensions
4. Remove anything suspicious or unnecessary

Mozilla Firefox

1. Click the menu button (☰)
2. Select **Add-ons and themes**
3. Review your extensions
4. Remove anything you don't remember installing

Quick rule of thumb:
If you installed it "just to try it once," it doesn't need to stay. Remove it.