

NAPLES COMPUTERS HOW-TO • SECURITY & SAFETY

How to Clean Up a Hijacked Browser

A browser hijacker changes your search engine or home page, adds toolbars, and floods you with pop-up notifications. This guide shows how to clean it up in Google Chrome (Microsoft Edge steps included): remove unwanted extensions, block site notifications, reset your browser settings, and check for unwanted programs. Example sites shown are fictional.

Step by step

WARNING SIGNS

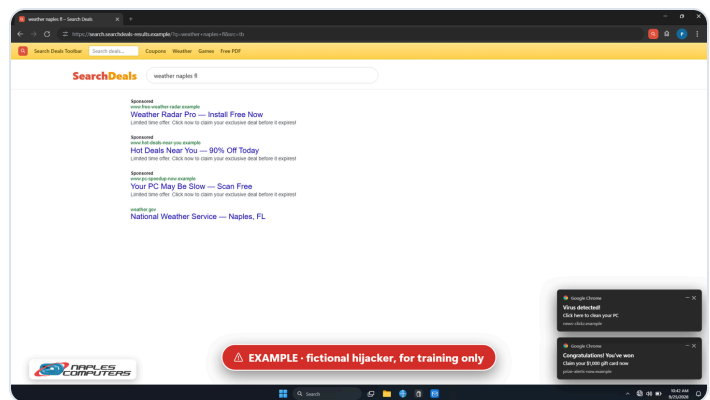


Signs your browser has been hijacked

Your search engine or home page changed, a toolbar or extension appeared that you didn't add, pop-up notifications show up in the corner, or pages keep redirecting to ads.

WHAT TO DO

Don't click the pop-ups, call any number, or install a "cleaner" they offer.

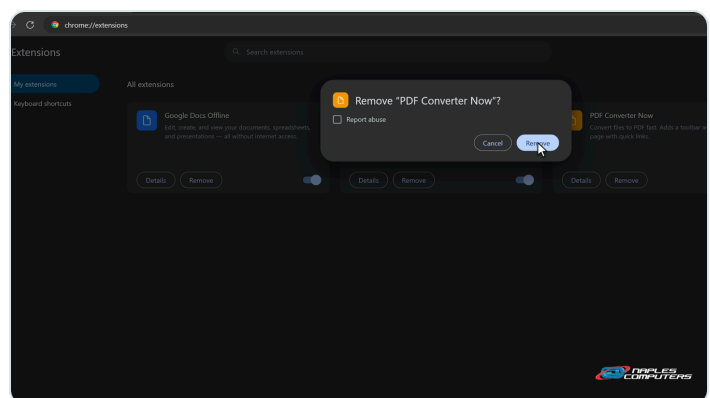


Step 1: Remove extensions you don't recognize

Chrome menu (:) → Extensions → Manage Extensions. Look for anything you didn't install on purpose.

WHAT TO DO

Click Remove, then Remove again to confirm. In Edge: menu (⋮) → Extensions → Manage extensions.



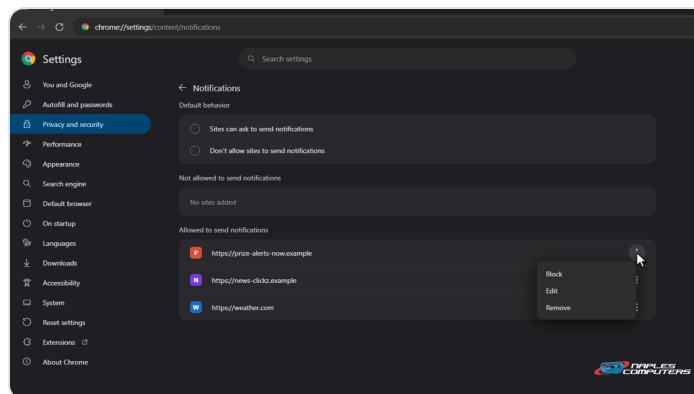
2

Step 2: Stop the pop-up notifications

Chrome Settings → Privacy and security → Site settings → Notifications. Find sites you don't know under "Allowed to send notifications".

WHAT TO DO

Click  next to the site and choose Block. In Edge: Settings → Cookies and site permissions → Notifications.



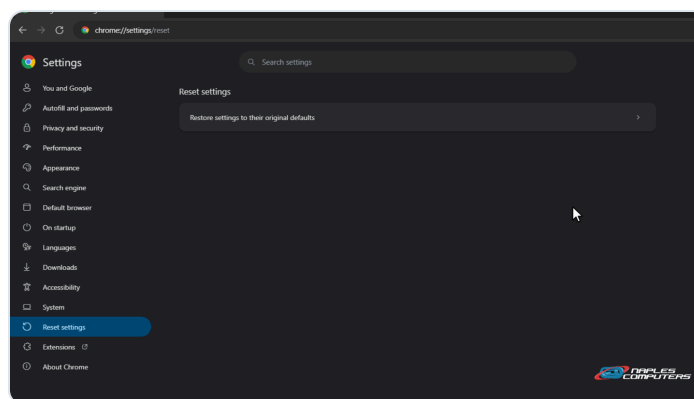
3

Step 3: Still acting up? Reset your browser settings

Chrome Settings → Reset settings → Restore settings to their original defaults → Reset settings.

WHAT TO DO

This resets the search engine, home page and startup tabs and turns off extensions. Bookmarks, history and saved passwords are kept. Edge: Settings → Reset settings → Restore settings to their default values.



Step 4: check for unwanted programs



Uninstall what you don't recognize

Settings → Apps → Installed apps, especially anything installed when it started



Run a full scan

Windows Security → Virus & threat protection → Scan options → Full scan



Get a second opinion

Malwarebytes has a free scanner

When to call a pro



It keeps coming back after a reset

Something on the computer is putting it back

- ☐ "Managed by your organization" on a home PC
A policy was installed that you didn't set up
- ☐ Pop-ups even with the browser closed
That points to a program, not just the browser
- ☐ You gave someone remote access or payment info
Call us, and call your bank. Change your passwords.

Business tip: lock down browsers

- ☐ Allow only approved extensions
Chrome and Edge policies, managed centrally
- ☐ Keep browsers updated automatically
Security fixes arrive every few weeks
- ☐ Filter dangerous sites
DNS filtering blocks many bad sites before they load
- ☐ Train your team
Never click Allow on notification prompts from unknown sites

Recap: clean up your browser

- | | |
|--|---|
| ☐ Don't click, call, or install | ☐ Reset browser settings |
| ☐ Remove unknown extensions | ☐ Scan for unwanted programs |
| ☐ Block site notifications | ☐ Still there? Call a pro |

Most hijackers ride in with "free" downloads or a click on Allow. Download software only from the maker's own site, and say Block when a site you don't know asks to send notifications. If it keeps coming back, we can remove it for you.



Browser still acting strange, or worried something got in?

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**