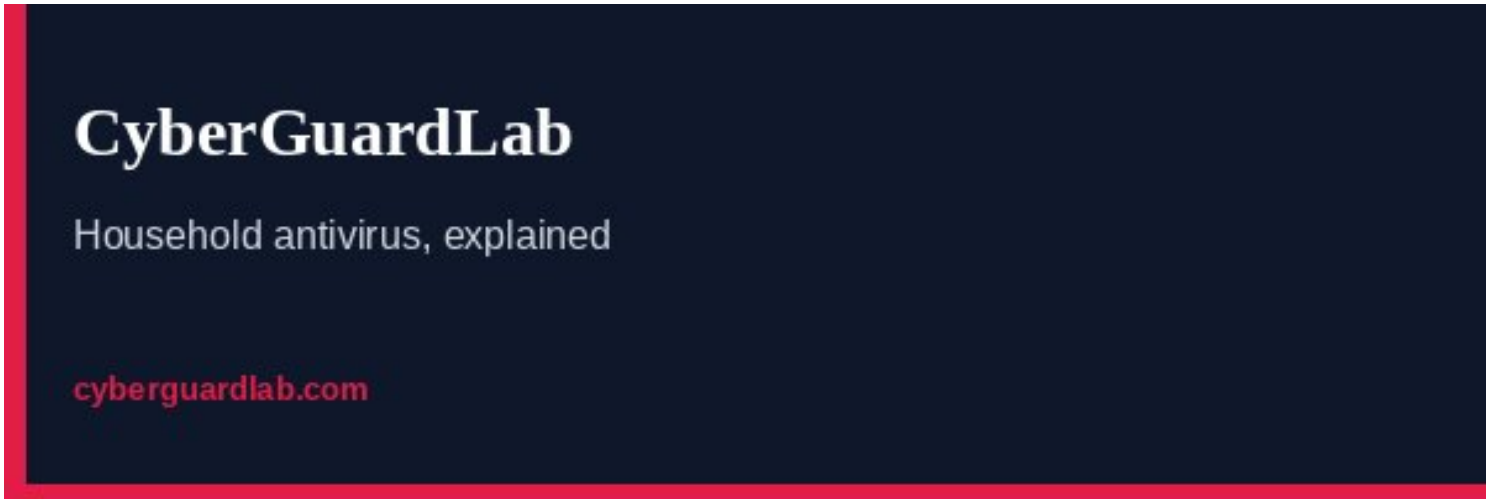
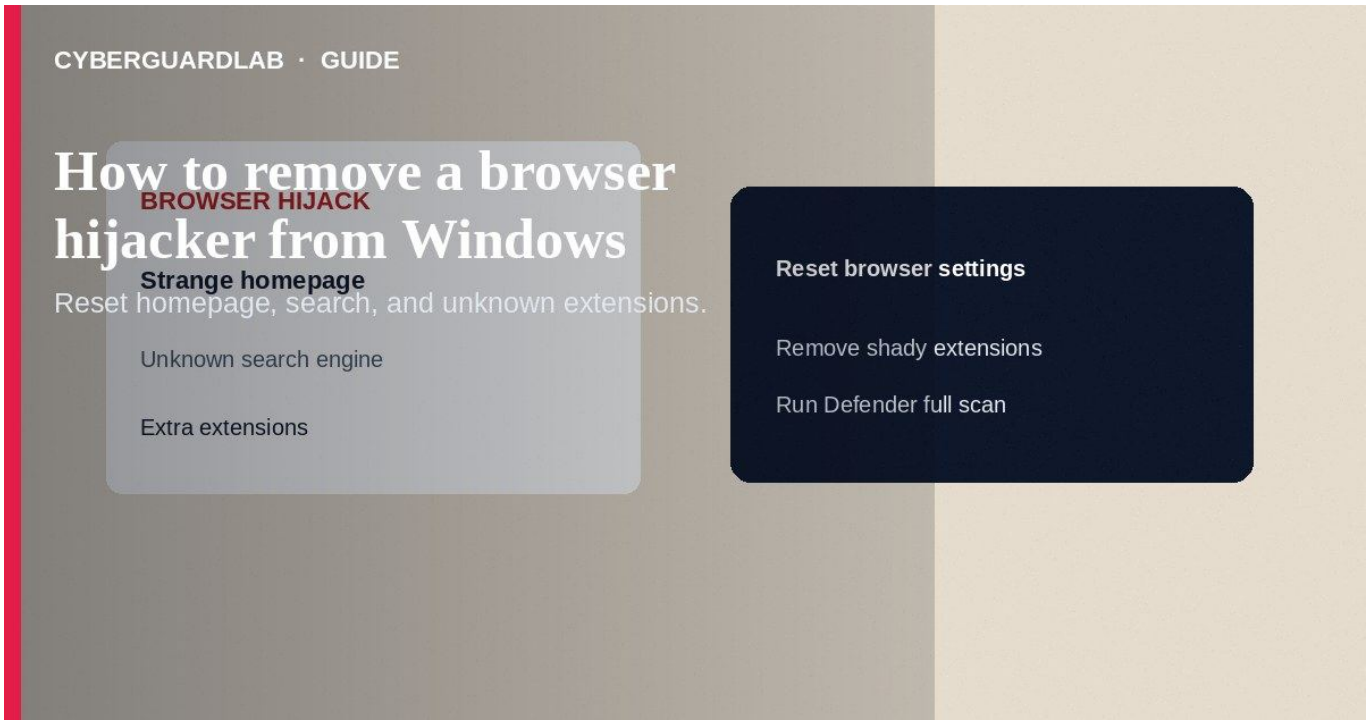


How to remove a browser hijacker from Windows

https://cyberguardlab.com/blog/remove-browser-hijacker-windows

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



A browser hijacker changes your homepage, default search, new-tab page, or extensions so ads and tracking pages open instead of what you chose-often after a bundled freeware install. Remove unknown extensions, reset the browser, uninstall shady programs in Windows Settings, then run a Defender (or trusted AV) full scan. This how-to is about hijacker cleanup on Windows-not a fake BSOD support scam, not a full Windows 11 keep-files reset as the first step, and not opening risky files in Sandbox.

1. Signs of a hijack

Searches redirect to unfamiliar engines; homepage keeps reverting; extra toolbars appear; pop-ups follow you across sites; new extensions you did not add show in the browser. Confirm whether SmartScreen or Defender already flagged related downloads.

Search results for "remove hijacker" are often filled with scareware. Prefer Microsoft's documented reset steps and Defender. If a page freezes with a support phone number, switch to the fake BSOD scam playbook instead of installing their tool.

2. Hijacker vs neighboring problems

Problem | Typical symptom | First move

Browser hijacker | Wrong search/home/extensions | Remove extensions; reset browser; uninstall PUPs

Fake BSOD support scam | Full-screen call-now scare | Do not call; kill browser; see scam guide

Keep-files reset | Deep OS corruption after malware | Use after cleanup fails; not first for a simple hijack

Risky unknown file | Untrusted attachment/download | Prefer Windows Sandbox before opening on the main desktop

3. Steps: remove the hijacker

* Disconnect briefly if redirects are aggressive; reconnect when ready to update definitions.
* In Chrome/Edge/Firefox, open Extensions/Add-ons and remove anything unknown. Disable first if unsure, then remove.
* Reset the browser settings to defaults (homepage, search, startup pages) from that browser's settings menu-use the official reset, not a third-party "optimizer" from a pop-up.
* Open Settings -> Apps -> Installed apps and uninstall toolbars, "search protectors," PDF helpers, or cleanup utilities you do not recognize. Restart Windows.
* Open Windows Security -> Virus & threat protection -> scan options -> Full scan. Quarantine detections.
* Check Task Manager -> Startup apps and disable unknown entries; review scheduled tasks if redirects persist.
* Change passwords for email and important sites if you typed them while hijacked (prefer another clean device).
* Keep one primary real-time antivirus. Norton or Bitdefender are common choices; TotalAV, McAfee, and Avast are other on-site comparison options-do not stack multiple full suites.

4. What to do if it comes back

* Re-check extensions after every browser update; some malware reinstalls helpers.
* Avoid "free codec / PDF / cleaner" bundles; use official Microsoft Store or vendor sites.
* If Settings and scans cannot hold a clean state, escalate to Reset this PC - Keep my files after backing up.
* Turn on reputation-based protection under App & browser control so SmartScreen can warn on unknown downloads.

FAQ

Is resetting the browser enough?

Often for extension-only hijacks. Persistently reinstalled PUPs need Apps uninstall + full AV scan.

Should I pay a pop-up cleaner?

No. Pop-up "PC cleaners" are frequently part of the scam. Use Windows Security or a suite you chose deliberately.

Does BitLocker stop hijackers?

No. BitLocker encrypts drives at rest; it does not remove browser malware while you are signed in. See BitLocker on a home PC for encryption, not hijacker removal.

Can I just create a new Windows user?

A new profile may avoid some per-user junk, but machine-wide PUPs remain. Still uninstall and scan.

If you still want a paid suite

Avoiding how to remove a browser hijacker from Windows does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* Microsoft Support: Tips for safer browsing in Microsoft Edge
* Microsoft Support: Reset Microsoft Edge settings
* FTC: Malware
* CISA: Understanding and protecting against malicious code

Also read

* How to spot a fake Windows blue screen support scam
* How to reset Windows 11 while keeping your files
* How to turn on SmartScreen for apps and files
* How to check Windows Security protection history
* How to check a download before opening an EXE