

How to Remove Browser Hijacker from Window 7

TechRounder PDF Edition

Live article: <https://www.techrounder.com/windows/how-to-remove-browser-hijacker-from-window-7/>

By Vipin PG | Published June 20, 2018 | Updated March 7, 2026 | Format: Guide | 4 min read

Quick answer

To remove a browser hijacker from Windows 7, uninstall any suspicious programs from the Control Panel, reset your web browser settings to default, and clear all browsing data including extensions and toolbars.

Are you are confronting an issue with your internet browser that continually diverts to a questionable site? At that point, there are chances that your Windows 7 is influenced by a browser redirect infection.

Indeed, the browser redirect infection is otherwise called Browser Hijacker. It targets Google along with other search engine tools to divert the client to shady and other contaminated sites.

In most circumstances, the diverted pages are packaged with a ton of infected commercials which influence the clients to pay something or give away their financial details. The essential capacity of these browser hijackers is to track the client's exercises and hack their information.

Presence of a browser virus is a clear sign of unwanted trouble. Along these lines, we recommend you expel the Redirect Virus from your Windows 7 PC. Follow steps introduced underneath to dispose of the Browser Redirect infection.

Working Methodology of Browser Hijacker Virus

Frequent redirects to shady and unsafe sites confirm the presence of Browser virus in your PC. It sneaks into your computer without permission bundled with freeware and shareware programs, through P2P sharing and torrent files, from contaminated web links available online, spam emails and sites giving free download offers.

Post successful installation on your Windows 7 system it sits silently in the background and alters the working of the pre-installed security system to avoid detection.

(Also see: [Avast Secure Browser - Best Google Chrome Alternative](#))

Once you have a compromised system, it changes the default settings of your web browser, redirects search results to the third party sponsored pages, displays an array of annoying ads on your computer system and track browsing history.

Its harmful effect degrades your browsing experience entirely and is solely responsible for its unusual behavior.

Furthermore, it is also capable of stealing and sharing your personal and confidential information with remote hackers. Personal information includes bank details, credit card information, personal security number, login credential and many more.

Why is Browser Hijacker Virus Harmful?

There is no denial of the fact that a browser virus can bring down your surfing experience. Let's here investigate the most noticeable impacts of this malevolent malware.

- Redirects search results with multiple sidetracks to shady and supported sites.
- Pop-up banners and undesirable promotions filling your PC screen based on your browsing history and perusing design.
- It is capable of changing your default program settings with a complete disability to reestablish your browsers unique settings.
- Addition of suspicious toolbars and modules getting showed on your PC screen.
- It may likewise impair default program updates.
- It takes and shares your personal and non-individual information with third-party organizations.
- Frequent sidetracks to malevolent and untrusted locales.
- System issues like decreased speed and incessant framework crash.
- Disrupted web availability with reduced network speed.
- Screen freezing issues and framework close down issues.

(Also see: Gmail Updated its UI with New Stylish Material Design)

Prevention tips

For system security and data privacy, it is essential that you follow basis computing hygiene while performing your online tasks.

Precautionary measures and proper watchfulness arms your system against harmful threats to a great extent. Let's here take a close look at some of the standards that you should follow.

- Third Party Installation: The networking landscape is loaded with numerous free download offers. Avoid downloading software using links from unsafe and shady sites. Ensure that you only use reliable and legit web pages for all your downloading requirements.
- Pop-Up Blocker: Pop-up ads and software update notification are mostly fake and are loaded with harmful virus. Use an efficient pop-up blocker tool to block all such contamination sources.
- Regular System Backup: Having a system backup lessen the impact of virus attack to a great extent. Keeping regular data backup save your life to a great extent.
- Update System Software: Regular updates arms your system against all zero-day threats. It is advised that you keep updating your system to fill security gap and reduce system vulnerabilities.

In this era of advanced technology, the precautionary measure may protect your computer to a certain extent but does not offer complete safety from malicious malware.

Dealing with browser hijacker virus is a tedious and requires an efficient automated process.

Choosing a robust and efficient system protection system will do the trick for you and will shield your system against all the odds and harmful PC threats like Remove Shortcut virus.

Antivirus programs are sophisticatedly designed to scan, detect and remove the harmful virus from your computer and provides real-time protection to your computer.

Download the best antivirus for Windows 7 today and ensure 360-degree system security and optimal performance.

References

1. howtoremoveit.info - browser-hijacker - <https://www.howtoremoveit.info/browser-hijacker/>
2. howtoremoveit.info - remove-shortcut-virus - <https://www.howtoremoveit.info/remove-shortcut-virus/>