

# Browser hijacking

## What is browser hijacking?

Browser hijackers change the default homepage and search engine in your Internet browser without your permission. Some hijackers edit the Windows registry so that the hijacked settings are restored every time you restart your computer.

These are generally used to force hits to a particular website, as in the use of blackhat Search Engine Optimization (SEO), to inflate a site's page ranking in search results. Although these threats don't reside on your PC, they do affect your browsing experience.

## How do I know if my browser has been hijacked?



A seemingly endless barrage of ads pops up on your screen.



New toolbars or Favorites are installed that give you icons and links to web pages that you don't want.



Home page or other settings change on your computer. Links are added that point to websites that you'd usually avoid.






Your computer runs sluggishly. Malicious software can slow down your computer.

## PRO TIPS

1. well-updated antispymware or antivirus software will likely remove the hijacker.
2. Some spyware scanners have a browser page restore function to set the user's homepage back to normal or alert them when their browser page has been changed.
3. disabling of add-ons on your browser



## REFERENCES

-  [http://en.wikipedia.org/wiki/Browser\\_hijacking](http://en.wikipedia.org/wiki/Browser_hijacking)
-  <http://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf>
-  <http://www.microsoft.com/security/resources/hijacking-what-is.aspx>