What Is Browser Hijacking?

One of the most popular topics discussed on computer help bulletin boards is browser hijacking. In most instances, computer users want to know how to protect themselves from malicious intrusions and outside control.

Browser hijacking occurs when unwanted software on an internet browser alters the activity of the browser. Internet browsers serve as the "window" to the internet, and people use them to search for information and either view it or interact with it.

Sometimes companies add small programs to browsers without permission from users. The makers of hijacking software range from computer and software manufacturers to hackers — or any combination of the three.

The Impact and Risk

Unscrupulous individuals and organizations inject their software into browsers for several reasons:

- To steal information from users
- To spy on users
- To display persistent advertising
- To run a try-before-you-buy hard sell to a consumer

Sometimes hackers drop malware into browsers to take users to websites used to capture critical information about them. The data could include user IDs, passwords, full names, addresses, social security numbers, and even answers to security questions — mother's maiden name, etc. Cybercriminals then use the information to access accounts that users log in to on the internet. In some instances, they can obtain financial data and steal a user's money or identity.

However, it doesn't take a super criminal to install software in a user's browser. Some marketing companies take the same steps to follow activity on the internet to see the sites users visit and how long they spend on those web pages. They then either use the information themselves to target their ad campaigns or sell it to other companies that use the data to focus their marketing content.

Sometimes companies spend their advertising dollars on display ads that pop up on users' devices or on messages that "follow" users around the internet.

Websites selling goods or services are increasingly placing pixels in browsers, and those pixels aren't always removed, even after users respond to the ads or offers.

The most pernicious form of browser hijacking occurs when a vendor forces a new and unauthorized software program directly into the browser itself. The intruding application could take up a significant amount of space on the browser's toolbar.

The purpose is usually to get the user to buy a full version of some type of software, shop on a seller's website, or search using a specific query engine.
Malicious or not, the files inserted into browsers take up storage space and slow down processing speeds on computers. Users need to be persistent in cleaning these files from their systems.

How to Get Rid of a Browser Hijacker

Some antivirus software alerts users to the presence of adware and spyware, but some new malware could go undetected, or the security software might be unable to root out the intruder. In these cases, users have to reinstall their browsers to regain control of the interface.
In extreme instances, the hijacking program reinstalls itself in the browser, and users may have to erase the contents of their computer, install a fresh operating system and the most current browser version, and restore their personal files from a backup.

How to Protect Your Systems from Browser Hijacking

Protecting against browser hijacking is challenging. Frequent cleaning of directories with browser cookies and histories helps. It's also critical to install and maintain quality antivirus software to stop malware from installing itself onto browsers. The security software should alert users to unauthorized installation attempts and ask how to proceed. This reduces the risk of infection.

Also, try to avoid running freeware programs, which upon installation may unpack software you’re unaware of. And be sure you check the download settings of any software you intend to install to reduce the chances of unwanted applications making their way onto your computer.
No matter which approach users take to protect themselves, the best defense starts with frequent operating system and browser updates and wise due diligence when visiting websites.

For more info visit:
https://www.kaspersky.com/resource-center/threats/browser-hijacking