How To Recover From Browser Hijacking

February 2020
By Phil Davis

Browser hijacking is when a program forcibly redirects your browser to a location that will produce some kind of monetary gain.

The software usually makes it onto your computer in one of two ways: Either a hacker tricks you into installing it via an email or a malicious link, or it's bundled with some legitimate software by a developer who uses it as an additional source of revenue.

If you've ever had your web browser hijacked, you know that it can be a pain to reset your browser so that it doesn't go back to the hijacking target.

It's important to periodically check to make sure your browsers are updated to the latest versions. Safari is usually updated at the same time as macOS is updated. Chrome and Firefox are updated automatically when you quit and restart the browser.

If you are the unlucky target of a browser hijacking, here are things you can do to return your computer to a healthy state.

Run Malwarebytes

The first thing is to run the Malwarebytes program, which can often find and remove the hijack program. Malwarebytes has both free and premium (paid) versions. When you first install the program, you get a limited trial of the premium version—it will revert to the free version after the trial period. Most people only need the free version, but you must remember to run it periodically.

After you run the program, reboot your computer. If this doesn't work, follow the instructions below.

Safari

Force Quit Safari

1. Click the Apple icon at the left end of the menu bar.
2. Select **Force Quit** from the menu.
3. Select **Safari** from the list.
4. Click the **Force Quit** button.

Remove Extensions

Some pop-ups are created from extensions and add-ons installed on your browser.

1. Open Safari
2. Select **Safari > Preferences**.
3. Click the Extensions tab. Click on Uninstall for any extensions you don't recognize.
4. You will get a confirmation window. Click on Uninstall to confirm the removal.
5. If a new tab opens up, you can close it by hitting the X.

Extensions are gone, but you may have to restart your browser for it to take effect. If you removed a malicious extension, it might have changed your homepage.

Modify Homepage Settings

Your web browser's homepage settings dictate the websites that load when it opens. If you see an unfamiliar link in the settings that should be removed, then follow these steps.

1. Open Safari.
2. Select **Safari > Preferences**.
3. Select **General**. 1. Set Safari opens with: **A new window**. 2. Set New windows open with: **Empty page**. 3. Set New tabs open with: **Empty page**.

Chrome

Open a Specific Page

1. Open Chrome.
2. Select **Chrome > Preferences (Settings)**.
3. Scroll down to the **On Startup** section.
4. Enable the **Open the New Tab Page** option.

You may want a specific page set to open by default. In that case, select the **Open a Specific Page or Set of Pages** option instead.

Reset Chrome Settings

Note: Resetting Chrome disables extensions, deletes cookies, removes pinned tabs and reverts home pages and search engine settings to their default. However, your bookmarks, browsing history, and saved passwords are still kept intact.

1. Open Chrome.
2. Select **Chrome > Preferences (Settings)**.
3. Scroll down and click **Advanced > Reset Settings**.
4. Click **Restore Settings to their original Default.**
5. On the pop-up box, click **Reset settings**. You have an option to **Help make Chrome better**.

Reinstall Chrome

If resetting Chrome doesn't work, it's time to reinstall the browser. This removes all data, including bookmarks, browsing history, and saved passwords. So, you may need to consider signing into Chrome and syncing them to your Google Account.

Note: Click the Sync option within the Chrome Settings screen and select the items that need to be synced, before removing the browser.

1. Uninstall Chrome completely using AppCleaner (free) or CleanMyMac X. If you just drag the Chrome icon to the trash it will leave several supporting files that must be deleted.
2. If you use **drag to trash**, you must remove any remaining files that have been left behind. To do this:
    1. In the Finder Menu, click **Go** and then **Go to Folder.**

2. Enter ~/Library/Application Support/Google/Chrome.~
3. Click **Go**.
4. Select all the folders, and drag them to the Trash.

Firefox

Force Quit Firefox

1. Click the Apple icon at the left end of the menu bar.
2. Select **Force Quit** from the menu.
3. Select **Firefox** from the list.
4. Click the **Force Quit** button.

Block Phishing and Malware.

1. Open Firefox.
2. Select **Firefox > Preferences** from the menu bar.
3. Select **Privacy & Security**.
4. Change **Browser Privacy > Enhanced Tracking Protection** to **Strict.**
5. Check all the boxes in **Browser Privacy > Security > Deceptive Content and Dangerous Software Protection**.

Disable Add-ons

1. Click **Tools** at the top of your browser window and select **Add-ons.**
2. Look through the list of add-ons and disable any you no longer use or do not remember installing.
3. Highlight the add-on and click the blue slider on the right to disable it.
4. To remove it completely, click the 3-dot icon to the right of the blue slider and click **Remove**.

Update Firefox

1. From the opened Firefox browser, pull down the Firefox menu and choose **About Firefox.**
2. Click the **Update Now** button if it's available, if you see **Firefox is up to date** then you're already on the latest version.

Final Thoughts

If none of these tips work, then it is time to either:

1. Restore your computer from a bootable clone backup made before the problem started;
2. Wipe your drive using Recovery Mode and Disk Utility, then reinstall macOS. Obviously you will need a good Time Machine or Bootable Clone backup to keep from losing everything.