(Approx. 1104 words)

How Do I Remove a Virus from My Browser?

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club
www.scscc.club

dkretch (at) gmail.com

Our computer operating systems have become more secure, so developers of malware have turned their attention to a more vulnerable target, our web browsers.

Chrome, Edge, Firefox, Safari, and Opera are the browsers most of us use to connect to the Internet. All of these browsers can be infected by a redirect virus, despite their built-in security.

Redirect viruses, also known as hijackers, can make your online life very difficult

In this article, I’m going to describe the process of acquiring, identifying, and removing an infection from your browser. I’m going to focus on Google Chrome; the techniques are similar, yet slightly unique for each browser. Most users should be able to use the described procedures on their own systems, with small variations depending on the browser and underlying operating system (Windows, Apple, or some flavor of UNIX/Linux).

Redirect viruses can come from several sources.

## Extensions

Hijackers can sometimes be “Trojan Horsed” in with browser extensions; extensions are small programs for a browser that serve the desired purpose, such as weather, price comparison, coupons, or productivity tools. If you install these extensions, you could unknowingly grant them the ability to influence your browser settings or change your preferences such as your home page or your default search provider.

Extensions are usually the first place to examine if you suspect you might have an infection.

## Spam emails

On at least a weekly basis I receive an email telling me that my account at Amazon, Facebook. eBay, PayPal, etc. have been frozen due to suspicious activity. The email contains a link to click on to resolve the problem. In reality, if I clicked on the link provided, my problems would be just starting. If you receive an email informing you of a problem with, for instance, your Amazon account, access your Amazon account the way you would normally if you think theremight be a problem.

## Social Media

Links from your Facebook or Twitter feed could also be rerouted in phishing, redirects, or browser hijacking. Facebook is notorious for allowing questionable items to appear in your feed. Some bad links might be posted by unsuspecting Facebook friends who find it easier to copy and paste or just click Share than to vet an item. And no, Costco is not going to send you a $50 voucher if you just take this survey revealing all sorts of personal information.

## Free software downloads from unreliable sites.

Hijackers can get added along with free software downloads. Often web sites will offer a desirable program but try to trick the user into downloading malware. Always look at the address bar to make sure you are downloading software from the legitimate provider’s site.

Without realizing it, you could lose control of your browser by clicking on the wrong link on the wrong website.

## Do I have a browser virus?

A browser virus on a PC or Mac is a browser hijacker that targets your browser. This type of malware is used to generate web traffic and collect information.

How do you find out if your browser has a virus? Here are the main symptoms:

* Your homepage redirects to a website different from what you expect.
* Unwanted extensions appearing in your browser (you might see icons at the top right side of your browser).
* Ads show up more often than they should, usually in unexpected places.
* Pop-ups and banners that advertise fake updates or software regularly appear.
* The link you click in search results redirects to dubious or possibly malicious websites.
* Your browser performance decreases dramatically no matter where you go on the Internet.

A virus can also ask you to update a program such as Adobe Flash Player or download any other tool (program) that would help you fix the problem it is creating. These warnings don’t always mean that you have issues with the browser but should be suspect.

If you notice any of these signs, your computer browser is possibly infected with a virus.

## Potential risks of a browser virus

As a browser hijacker, a pop-up virus is categorized as a potentially unwanted program (PUP). Once the malicious program attacks your computer, it starts modifying browser settings. For instance, it changes the default search engine and homepage, without asking for your permission.

The most serious problem created by having this virus is the ultimate invasion of your privacy; secretly harvesting as much of your personal information as possible to engage in identity theft. Some browser viruses are all about collecting personal details (IP address, location, searches, etc.) and sharing them with third parties. This may cause serious problems related to privacy and data security.

## How to get rid of the browser virus

**Delete unrecognized extensions**

1. Go into your browser settings (in Chrome it is the three perpendicular dots at the upper right side of the browser).
2. Click on the Extensions tab.
3. Look for any extensions that shouldn’t be there. If you find anything, select it and hit the Uninstall button to remove it.

**Check your homepage and search engine settings**

These settings appear in the settings area of your browser. In Chrome go into the browser settings and click on Settings. Make sure your homepage and default search engine are correct.

**Additional things to check**

1. Go to the Applications or Applications and Features folder and find any suspicious software. It may disguise as the desired application, so search for anything you don’t remember downloading. Also, note the install date to identify possible problems and look at the last program you downloaded before noticed problems.
2. Check your Downloads folder for items recently downloaded from the Internet for clues about the possible problematic vector that has introduced the malware into your browser.
3. Once you detect the malware, drag it to Trash and empty it, or delete it and then remove it from your Recycle Bin.

**Get rid of every trace of malware**

After the above steps, download and perform a Malwarebytes scan as well as a full scan with your installed virus protection to make sure no harmful PUPs are left on your system.

## Conclusions and Recommendations

To avoid getting browser viruses, pay attention to the websites you visit, files you download, and apps you install. Avoid using third-party software downloaders and installers - they usually include PUPs. Never ignore the warnings if your browser alerts you that a website is not secure.

Still, it’s always better to prevent the problem than to try to deal with it. Browse wisely!

