



Computer Hijacking... What Happened to my Homepage?

Question: When I startup my computer my homepage switches to a site that I don't want. No matter what I do I can't make this problem go away. What can I do?

Answer: Uh oh, your browser has been hijacked. Some Internet company out there has put a little program on your computer that switches your homepage every time you either restart your browser or your computer. Not nice.

The good news is there are ways to fix the problem.

First here's the normal way of changing your browser's homepage. At the top of Internet Explorer, click Tools then Internet Options then change the Home page address and click ok. In Netscape 7, click Edit then Preferences and then change the homepage address in the box that appears.

If you've been hijacked this won't work for long, because the rogue programming on your computer will soon change it back. So how did this happen?

Well from a programming perspective here's what's happened: The most common scheme used by homepage hijackers is to put a reference to their site in your Startup folder or Registry Run key, so that it runs every time the computer is started and changes your settings. If you try to change any of these back, the programming they put on your computer changes everything so you end up with their site in your browser.

The only way to fix this is to find the hijacking software and remove it.

"But I didn't download anything to allow this happen!" you might say. Well, if you don't regularly update your browser or use Windows Update to install security fixes, then you did. Several of these hijackers exploit an Internet Explorer/Outlook Express bug that lets them secretly install a program (called an ActiveX control) on your system just by viewing their Web page. Hijackers exploiting this bug will insert one or several .hta files on your hard drive which run when you start up Windows.

To fix this nastiness, search your computer for *.hta files. Click Start and Search or Find and then Files or Folders and type in *.hta. If you find them rename them so that they can't be found. For example, change **file.hta** to **file.hta1** or move the files to another folder on your computer. Then switch your homepage back to one you like. If your computer doesn't do weird things after this permanently delete them. If it does, you might want to put them back one by one until you find the offender and then delete it.

Also, don't forget to grab the Microsoft patch which fixes the browser hole that allows the hijacker to work this little piece of dark magic.

To get the fix, run Windows Update found on your START menu .

Some hijackers, like Gohip, install an executable program (ending in .exe, something like hijack.exe) on your your computer. Since .EXE programs can't be automatically downloaded in the secure browsers (with all the latest security fixes installed), you usually get this by downloading a program from the web.

Hijackers sometimes mark these programs as "browser updates" or "browser enhancements" or some other trickery. The hijacker typically offers you all kinds of incentives (freebies, special deals and stuff like that) to install the evil program.

Also see Lavasoft's free **Ad-Aware** which removes spyware from your system for free: www.lavasoftusa.com

Finally, there's another hijacking method. Some sites will find a way to put a shortcut in the Windows Startup folder or Registry Run key that starts the Registry Editor (regedit), then tells it to add the contents of a hidden file (e.g. C:\windows\temp\abcdefg.tmp) that contains the necessary information to set the hijacker's homepage to the Registry on every startup.