How to remove PublicBoardSearch browser hijacker

According to the infection method, PublicBoardSearch belongs to the type of browser hijacker. This is a type of malware designed to take up the settings of a familiar browser.

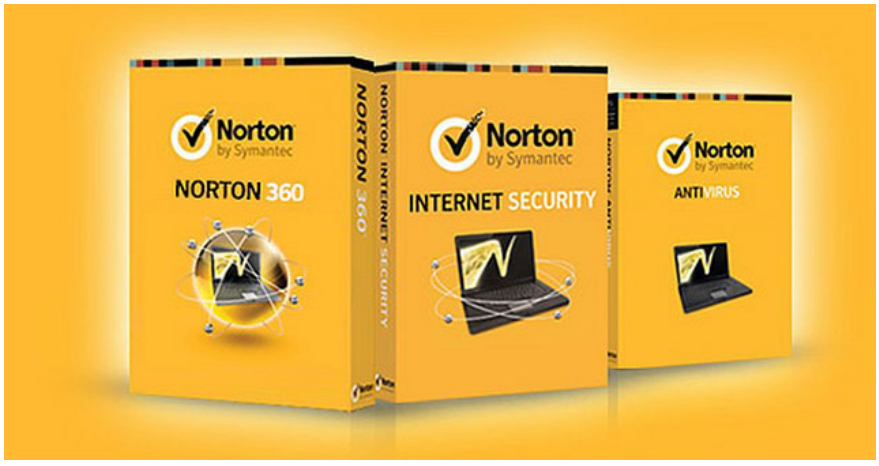
What is PublicBoardSearch?

According to the infection method, PublicBoardSearch belongs to the type of browser hijacker. This is a type of malware designed to take up the settings of a familiar browser. This means that from now on the browser will be under the control of the virus. For example, any request in search engine will now be redirected to other fraudulent websites without your consent.

In addition, the virus will provide the device with continuous advertisements for you to accidentally click and go to dangerous sites. In general, scammers benefit from user views and visits to dangerous sites that harm the system. PublicBoardSearch needs to be removed as soon as possible.

How to remove PublicBoardSearch browser hijacker

1. Automatically remove PublicBoardSearch browser hijacker



The simplest method to stop Mysearch-app.xyz ads is to run an anti-malware program capable of detecting adware in general and Mysearch-app.xyz ads in particular.

Norton is a powerful antivirus software that protects you against malware, spyware, ransomware, and other types of Internet threats. Norton is available for Windows, macOS, iOS, and Android devices.

2. Removed the PublicBoardSearch browser hijacker from Programs and Features

Go to **Programs and Features** , uninstall suspicious programs, programs you don't remember installed, or programs you installed right before the PublicBoardSearch browser hijacker appeared on your browser for the first time. When you are not sure if a program is safe, look for the answer on the Internet.

Refer to the article: 7 ways to remove software, delete applications on Windows computers for detailed instructions.

3. Remove the fake program from File Explorer

This step is intended for an experienced computer user. You may accidentally delete something that you shouldn't do.

Sometimes malicious programs don't show up in **Programs and Features** . Check **% ProgramFiles%,% ProgramFiles (x86)%,** especially **% AppData%** and **% LocalAppData%** (these are shortcuts. Please type or copy and paste them into the File Explorer address bar).

If you see folders with strange names, look inside, Google those names to find out if they belong to legitimate programs or not. Delete the folders that are definitely related to the malware. If you are unsure, back them up before deleting (copy to another location, such as to a USB).

4. Remove the PublicBoardSearch browser hijacker from the browser

Remove any suspicious extensions or extensions that you do not recognize from your browser. Reference: How to remove Add-ons (Extensions) on Chrome, Firefox and some other browsers for more details.

5. Clear PublicBoardSearch browser hijacker message

Remove the PublicBoardSearch browser hijacker message from Google Chrome

1. Open **chrome: // settings / content / notifications** (just copy and paste in Chrome's address bar).

2. Remove all fake notifications by clicking the three vertical dots button next to each notification and selecting Remove.

6. Remove the PublicBoardSearch browser hijacker message from Mozilla Firefox

1. Click the menu button and select **Options.**

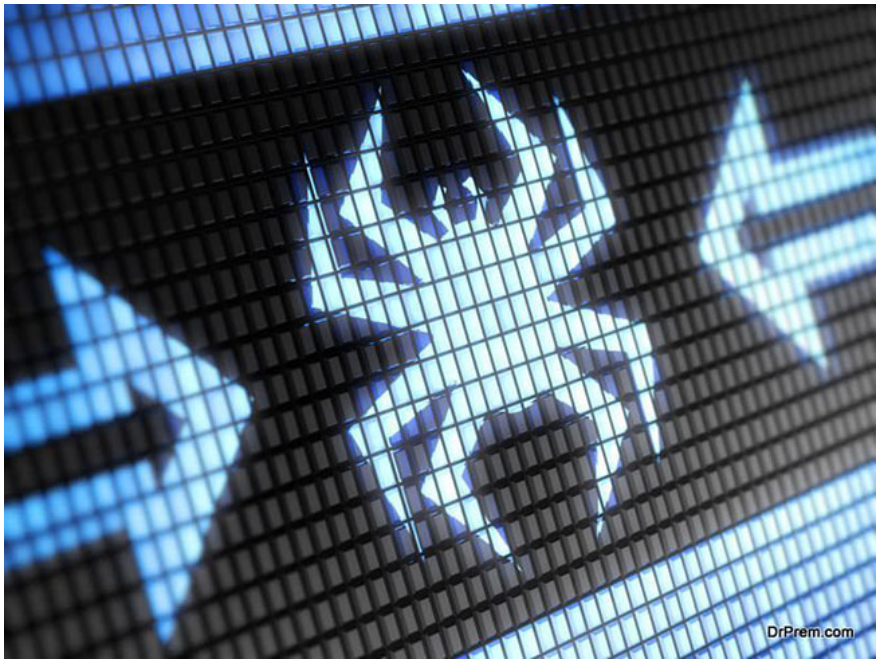
2. Select **Privacy & Security** on the left side of the window.

3. Scroll down to the **Permissions** section and click the **Settings…** button next to **Notifications.**

4. Find the websites you don't want to see notifications for, click the drop-down menu next to each page and select **Block.**

5. Click the **Save Changes** button **.**

How to protect your PC from the PublicBoardSearch browser hijacker



1. Install a powerful anti-malware program capable of detecting and removing PUPs. Having a few on-demand scanners would also be a good idea.

2. Always turn on Windows Firewall or get a third party firewall.

3. Always keep your operating system, browser, and security utility up to date.

Malware creators always find vulnerabilities in new browsers and operating systems to exploit. The software writer will then release patches and updates to remove known security vulnerabilities and reduce the risk of malware invading. Antivirus program signature database is updated daily and even more often to include new viruses.

4. Adjust browser settings to block pop-ups and load plug-ins only when clicked.

5. Download and use the uBlock Origin, Adblock, or Adblock Plus browser extension / add-on to block third-party ads on websites.

6. Don't click on any links you see while browsing, especially links in comments, on forums or in instant messaging tools. Usually these are spam links. They are sometimes used to increase traffic to websites, but they can lead you to sites that will try to execute malicious code and infect your computer. Links from friends should also be suspicious: The cute video sharer may not know that the page contains something malicious.

7. Do not download software from unverified websites. You can easily download a trojan (malware pretending to be a useful application); or some unwanted programs can be installed with the application.

8. When installing freeware or shareware, be cautious and do not rush in the process. Select **Custom** or **Advanced** installation mode **,** find checkboxes asking you to allow third-party applications to be installed and uncheck them, read the End User License Agreement to make sure that nothing else will be installed.

Of course, you can set exceptions for applications you know and trust. If you can't refuse to install the unwanted programs, the article recommends you to completely uninstall it.

You finished reading the article "**How to remove PublicBoardSearch browser hijacker**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.