How To Remove Browser Hijacker Virus From PC

Browser Hijacker is a harmful computer infection. It is capable of altering your web browser homepage and thus force you to click on particular websites for making profit. It may forcibly redirect your browser on harmful and malicious web pages from where your system can get some more threats. It is focused for making profit via unwanted redirection of web traffic. It is a cunning PC virus threat and thus malware researchers' advice the immediate removal of this threat.

Why Browser Hijacker Is Harmful

Browser Hijacker is an unwanted program that get into your system without permission. It is able to alter your main web browser every time you go online. It generates lots of unwanted redirections for making profit. It has main focus on redirecting the web traffic on third party websites to earn commission. Browser Hijacker pretends to be a genuine search engine. It can replace the homepage of your compromised browser. After that it will appear as the default start page whenever you launch your browser.

Browser Hijacker virus can also redirect your browser when you try to visit any specific website. It will show sponsored search results on your computer in order to boost the traffic of its partner websites. It can also generate lots of unwanted and misleading advertisements on your computer. Those annoying adverts can lead your browser on questionable and malicious websites where you can get some potential threats on your machine. It can also bypass the firewall and anti-virus program that makes the removal of this threat a bit tricky.

How Browser Hijacker Infiltrate Your PC

Normally **Browser Hijacker** virus get on your system bundled with free third party programs and software. Bundling is a completely legal marketing method to promote different types of programs online. Hackers also use this method to inject malicious codes and evil programs on the user's computer without their approval. You can also get this virus on your system when you browse to malicious websites or visit on porn links. It can also get delivered on your machine through spam email attachments.

How To Removal Browser Hijacker Virus

Removal of Browser Hijacker browser hijacker virus could be very tricky. This nasty threat can even dodge experienced users. It is possible to remove this threat manually from infected PC but it need some good computer knowledge. But if you are a novice user then you are suggested to use a powerful anti-malware application to get rid of this

nasty threat completely from your system. Browser Hijacker is a very destructive threat and you must remove this infection soon from your computer.

Malicious Doings of Browser Hijacker Virus

Browser Hijacker is a severe computer virus that can do major harm to your system. Once getting the access of your unharmed PC, it will start doing its malicious activities. Some of the most common mischievous activities Browser Hijacker virus start into your system

1. **Targets All Windows PC** : This dubious computer virus can infect all versions of Windows computer including Windows XP, vista, 7, 8, 8.1 and the latest Windows 10.
2. **Malicious code injection** : This perilous threat can corrupt your registry files and inject its malicious codes to the registry files for getting automatically started on your machine without your permission.
3. **Browser Redirection** : Browser Hijacker virus can also infect your working web browser and causes unwanted web redirection. This nasty threat can also bring other noxious malware on your PC.
4. **Data Corruption** : Browser Hijacker virus is a lethal PC threat that harm your entire system data. It can corrupt your files and programs. It can also cause black screen of death on your computer.
5. **Disable Security Programs** : This nasty PC infection can also block your anti-virus and Firewall program to make its self safe in to your machine for longer time.
6. **Gather sensitive Data** : It can also gather your secret and confidential information by using keylogger and tracking your browsing habits. It can also risk your privacy by sharing your personal information with hackers.
7. **Remote Access (Backdoor)** : Browser Hijacker is such a harmful virus that can allow remote hackers to remotely access your system. It can make your system more vulnerable and expose your privacy.

Possibilities to Remove Browser Hijacker Virus

It’s certainly possible to remove Browser Hijacker virus from your PC, however it’s not going to be an easy task at all. When it comes to remove this particular malware infection, users should know that there are two possible options to get rid of Browser Hijacker virus from Windows PC. Well, both possibility to remove this malicious threat completely from your system is been described below, take a look.

How to Remove Browser Hijacker From Your PC

Option A : Easily Remove Browser Hijacker Automatically With SpyHunter (Recommended)

Option B : Remove Browser Hijacker Manually From Your PC

Option A : Automatically Remove Browser Hijacker Using SpyHunter

The best and the easiest way to get rid of this nasty Browser Hijacker virus is to use SpyHunter Malware Scanner program. It is an effective and powerful malware removal tool that can easily delete any kind of harmful computer infection. This advanced and ultimate security software is able to ruin all kind of latest threats and malware. It can scan your system deeply to find out all possible and potential viruses.

Why SpyHunter?

SpyHunter is the best and powerful ant-spyware application that give real time protection to your computer. It is designed to assist you to remove all types on threats in few clicks. It is an optimum security suite which is configured to give best protection to your system with very less effort. All you have to do is to download and install this application on your system. Just start a scan of your PC and rest will be done by this program. SpyHunter is able to detect and remove all kind of rootkits, spyware, malware, threats, viruses, adware, browser hijackers, worms, Trojam, ransomware and many more.

User Guide :- Parts to Use SpyHunter To Remove Browser Hijacker

Step 1 - Download the **SpyHunter malware scanner** on your PC and run the installer.

Step 2 - Click on **Scan Computer Now** to start a new scan of your system.

Step 3 - SpyHunter will detect **all possible threats** on your machine.

Step 4 - Click on **"Fix Threats Now"** button to remove all threats and malware.

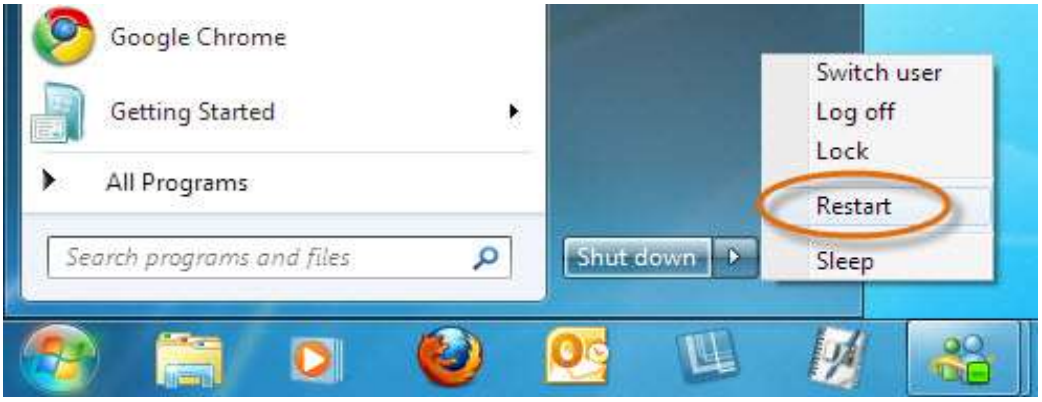
Option B : Remove Browser Hijacker Manually From Your PC

Risk Involved With Manual Removal Process

Well, manual removal option is good but only for computer geeks. Well, if you are not much technically sound then manual methods can prove quite risky for you as it is quite lengthy and complicated process. It has been seen that even minor mistake while using manual steps result in very critical consequences for users. If manual method goes wrong, then users can lose their important data and it can even make your system completely useless instead of removing Browser Hijacker virus.

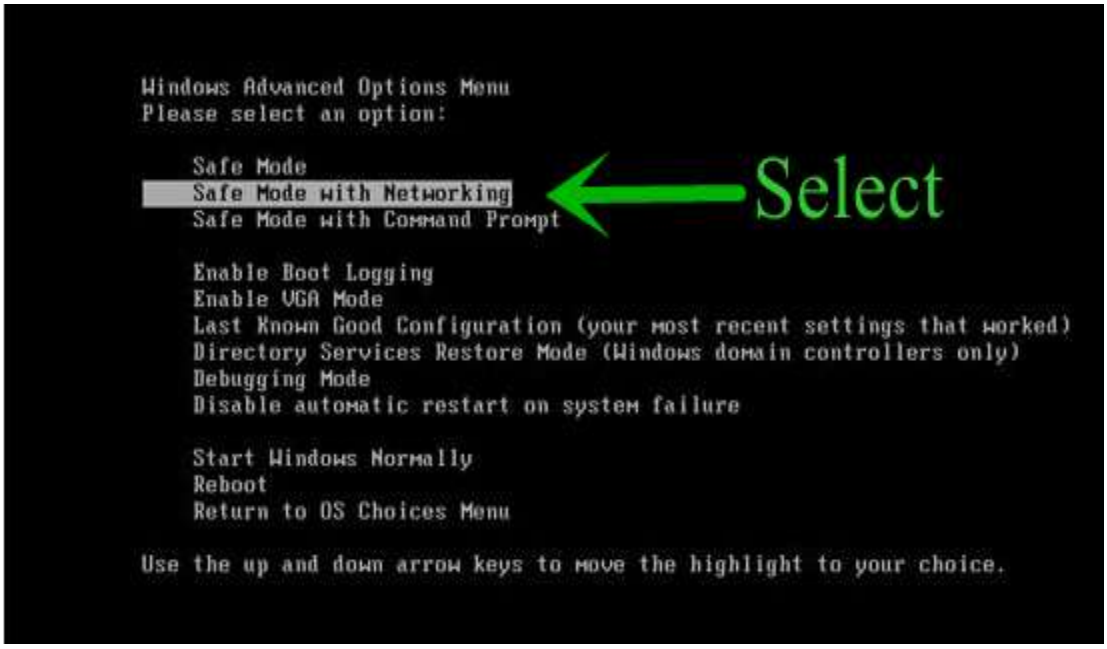
Part 1 :- Boot Your PC in Safe Mode

- **Restart** your Windows computer to open **boot menu**.



- Keep pressing **F8** button until **Windows Advanced Option** appears on your system screen.

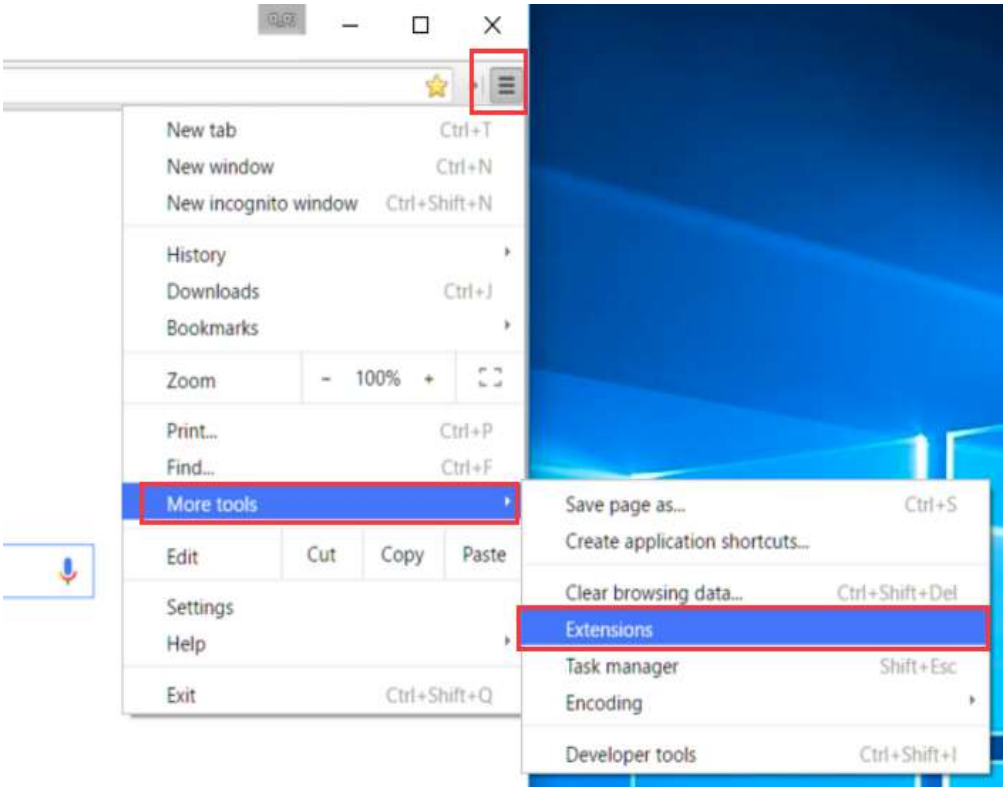
- Now **Select Safe Mode With Networking** Option using **arrow key** and press **Enter**.



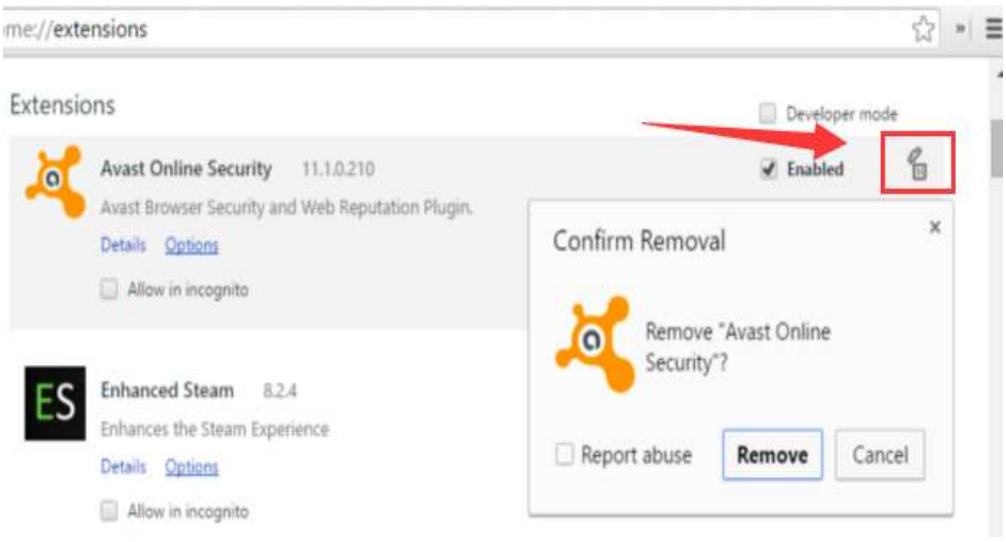
Part 2 :- Remove Browser Hijacker From Browsers

(A) : Remove Malicious Extension From Google Chrome

- Open browser ➡ click on **gear** icon (☰) ➡ Select **Tools** and then open **Extensions** option.

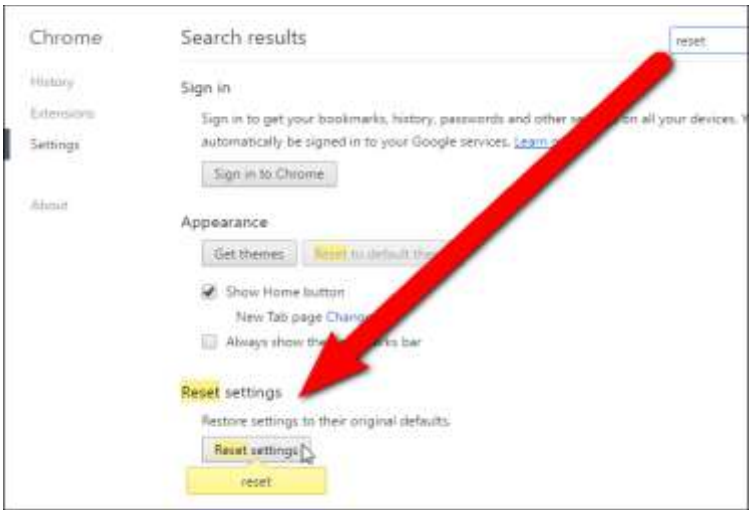


- From the List of all extensions select Browser Hijacker and then click the **Trash** icon to remove this malicious extension completely from your Chrome browser.

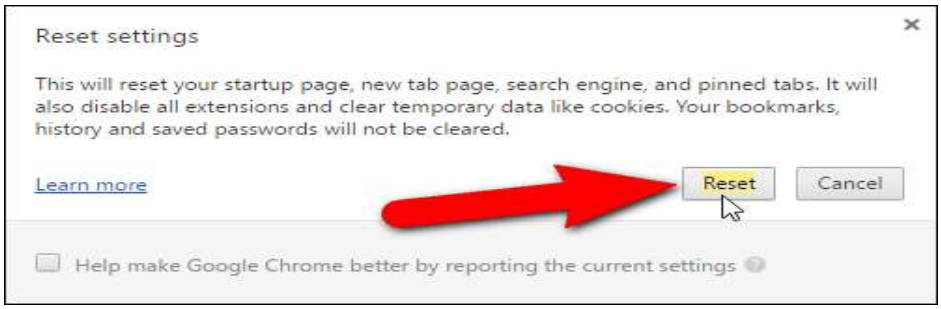


Reset Browser Settings

- Open **Chrome** ➡ click on **(☰)** icon ➡ choose **Settings** option and select the **Show Advance Settings**.

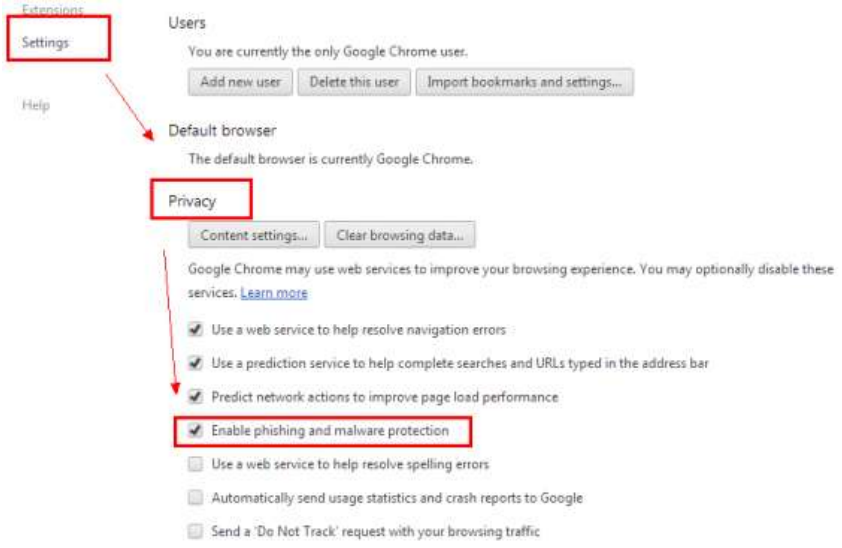


- Now go to the end of the page and click **Reset Settings** button.



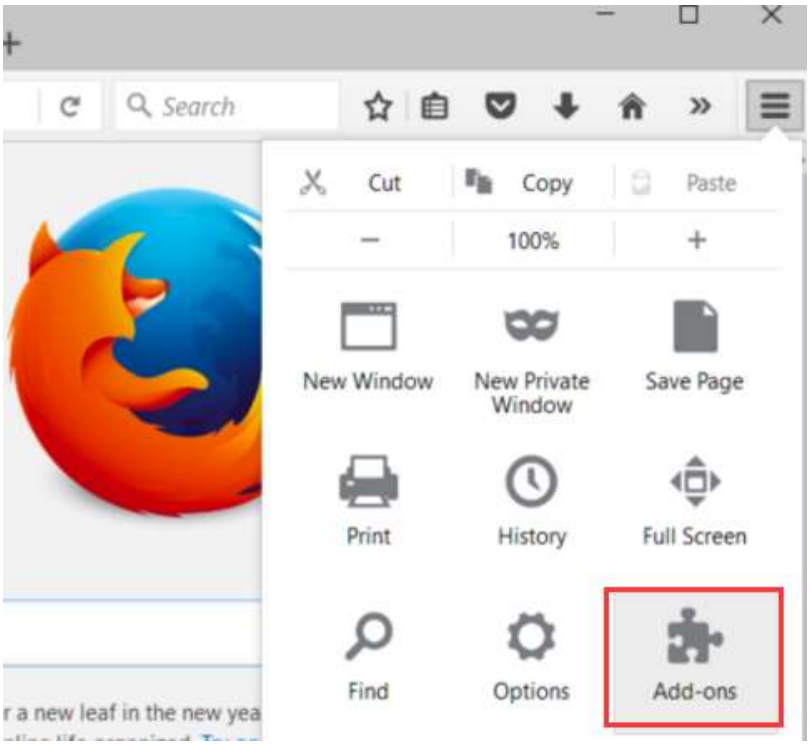
Enable Phishing and Malware Protection

Click on **(☰)** icon ➡ choose **Settings** ➡ **Show Advance Settings** and in **Privacy** section select **Enable Phishing and Malware Protection** option.

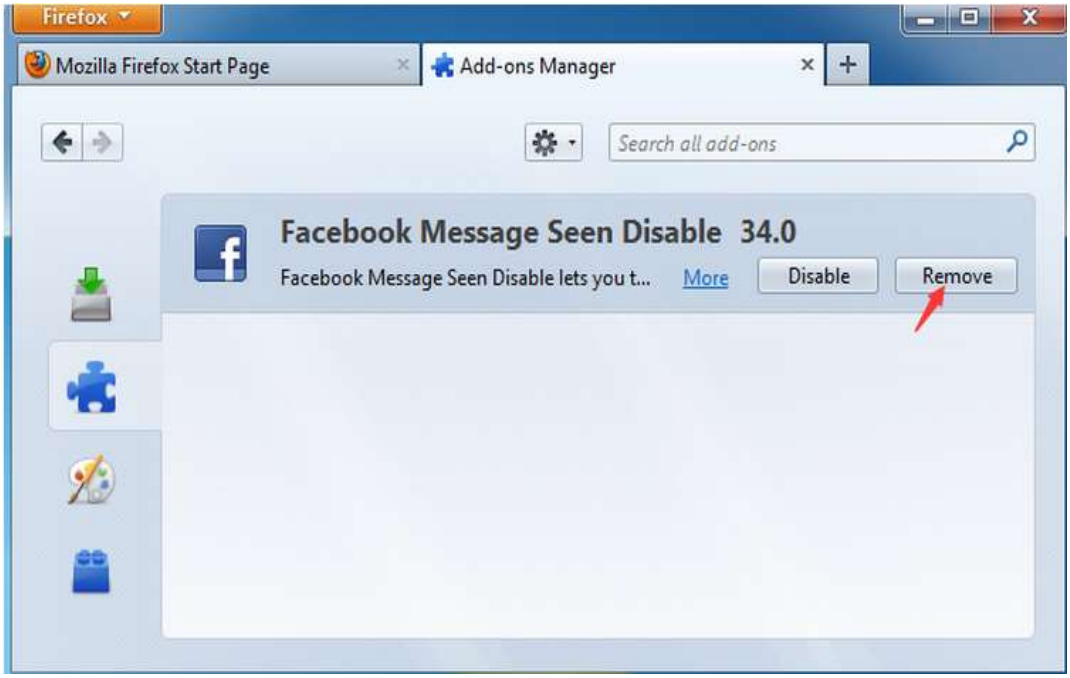


(B) : Remove Malicious Extension From Mozilla Firefox

- Open **Firefox** ➡ click **(☰)** icon ➡ select **Add-Ons** option.

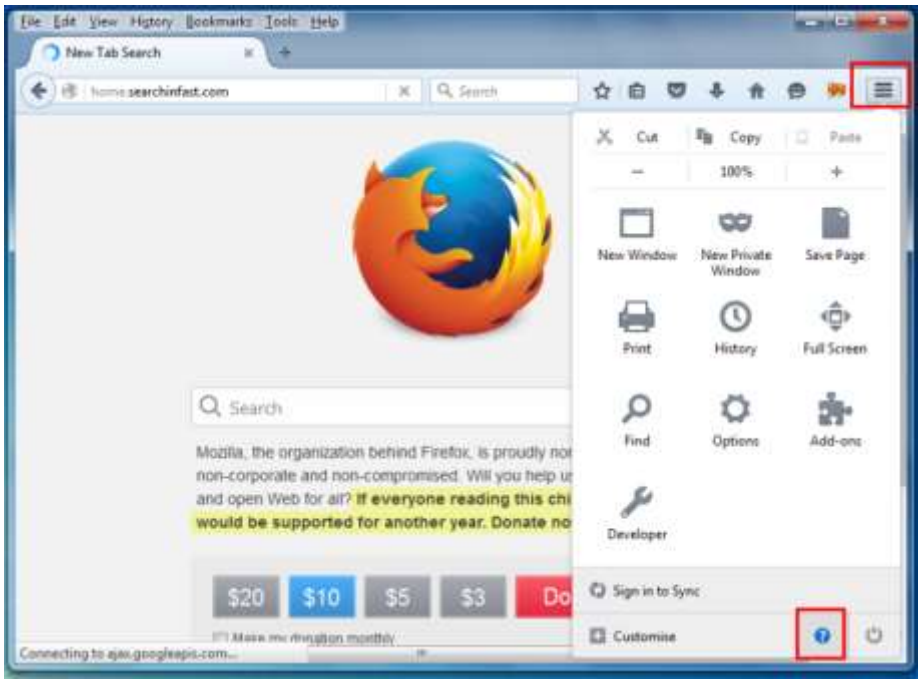


- Go to **Extensions** option from left panel. Select and remove all malicious extensions related with Browser Hijacker.

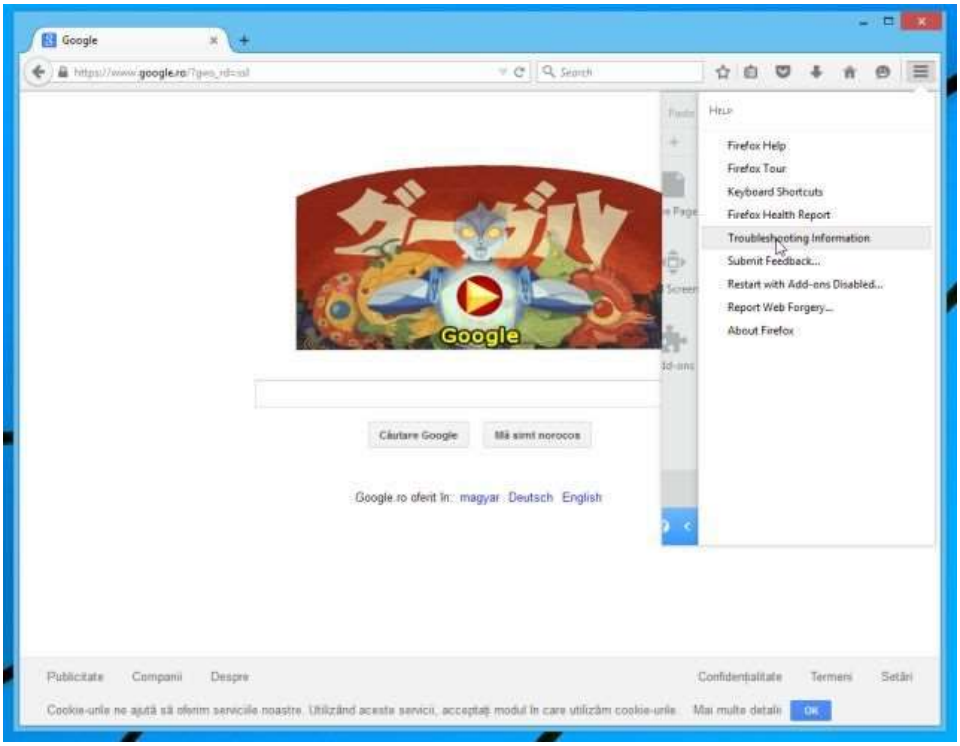


Reset Browser Settings

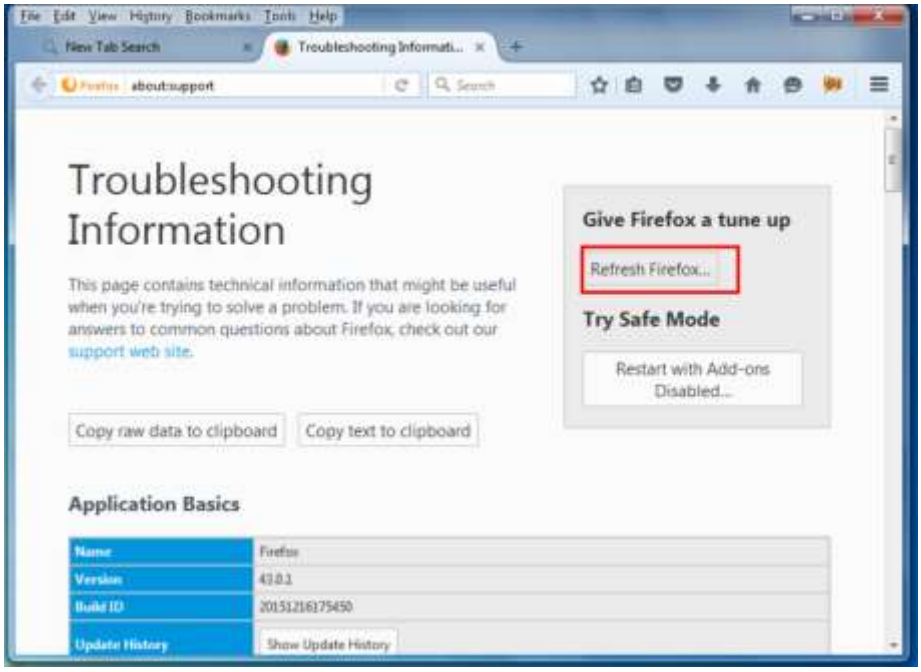
- From upper right corner of browser click **(☰)** icon ➡ **Help option.**



- Choose **"Troubleshooting Information"** option from the list.

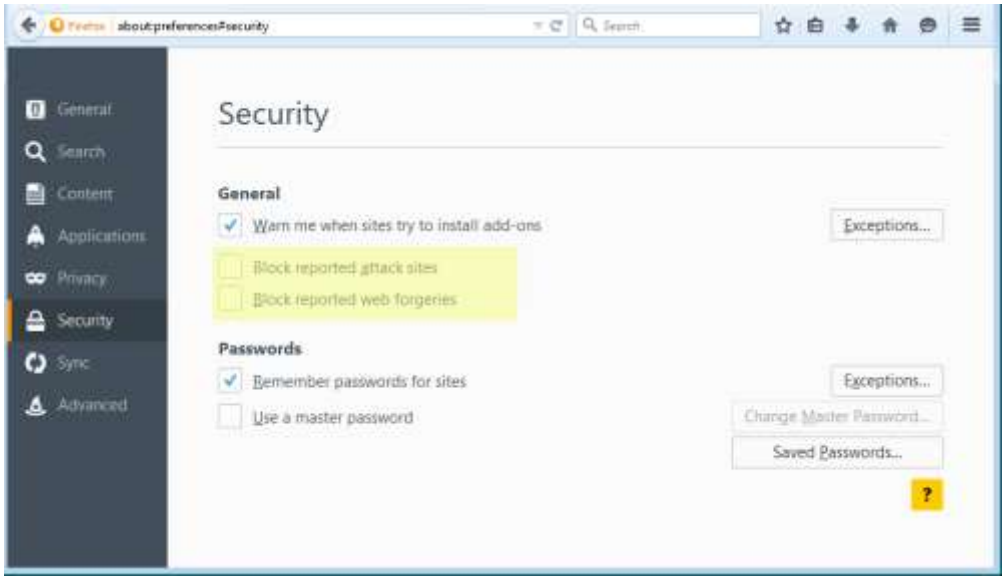


- Click **“Refresh Firefox”** button from Troubleshooting Information page.



Block Phishing and Malicious Website In Firefox

Open **Firefox** ➡ click **(☰)** icon ➡ go to **Option** Menu ➡ choose **Security** option and tick the following option.



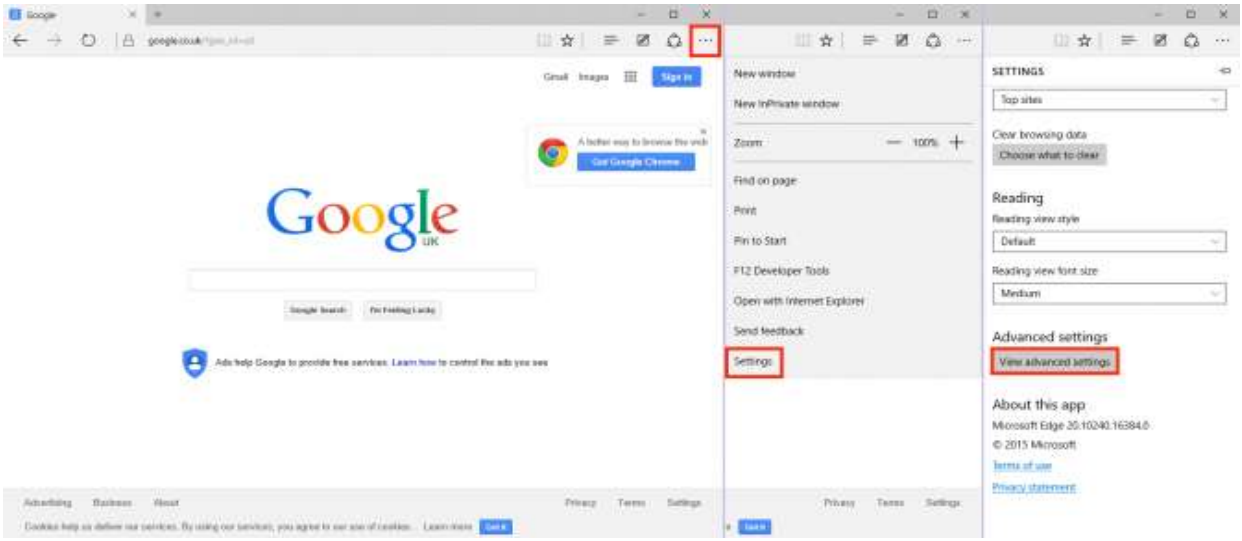
- Warn me when sites try to install add-ons.
- Block reported attack sites
- Block reported web forgeries

******What To Do With Microsoft Edge Browser******

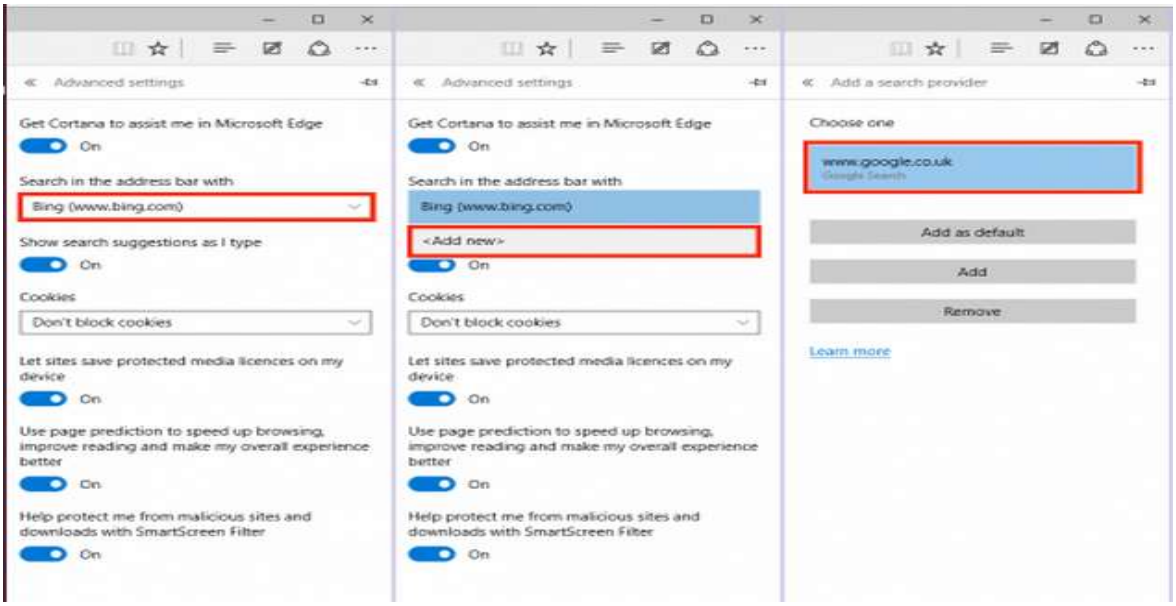
Since, Microsoft Edge browser does not have extensions option hence you should better reset your browser settings in order to remove Browser Hijacker from your web browser completely.

(C) : Reset default search engine and homepage

- From top right corner of your Edge browser Choose **More (…)** ➡ Go to **Settings** ➡ Click on **View Advanced Settings** option.

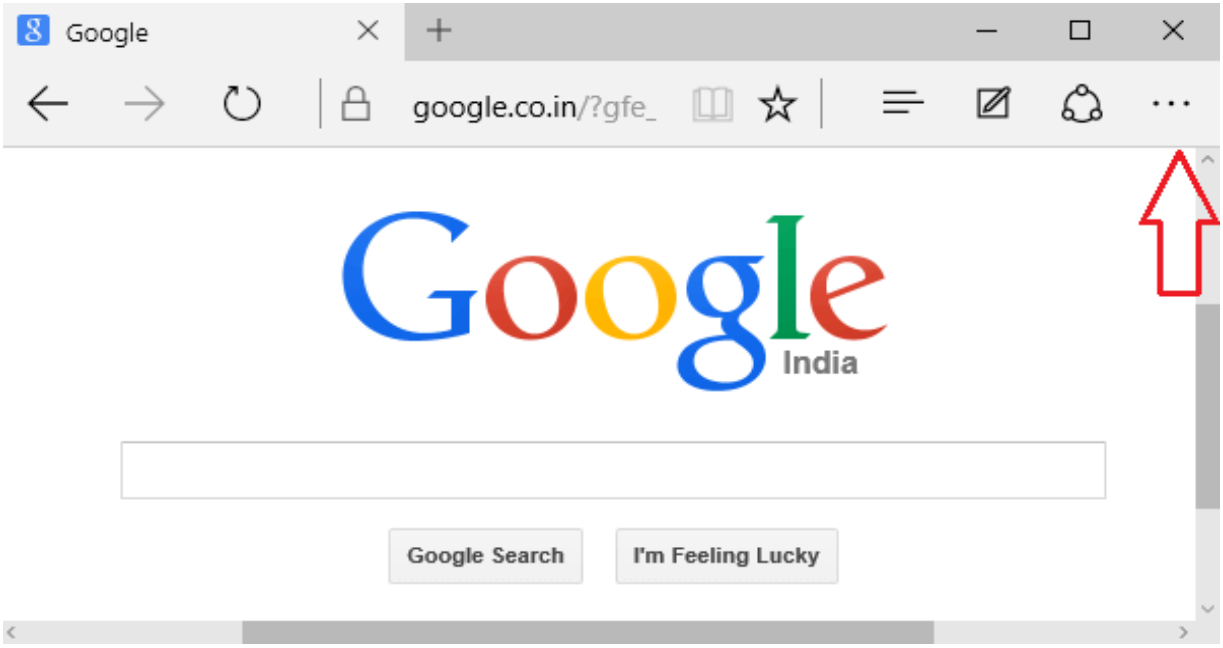


- Here, hit <**Add New**> ➡ **Add a search provider** option and enter desired search engine. Finally Click **Add as default** to reset your browser search engine.

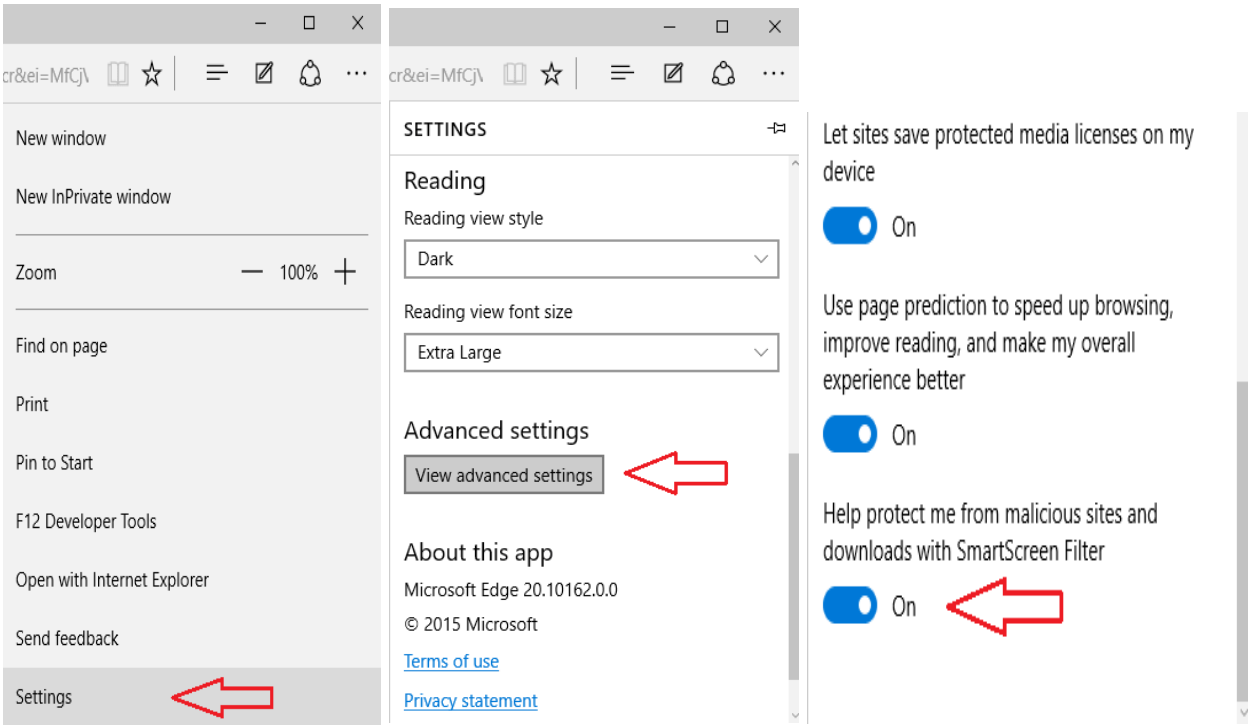


Enable SmartScreen Filter in Microsoft Edge

- Open browser ➡ click **(…)** icon.

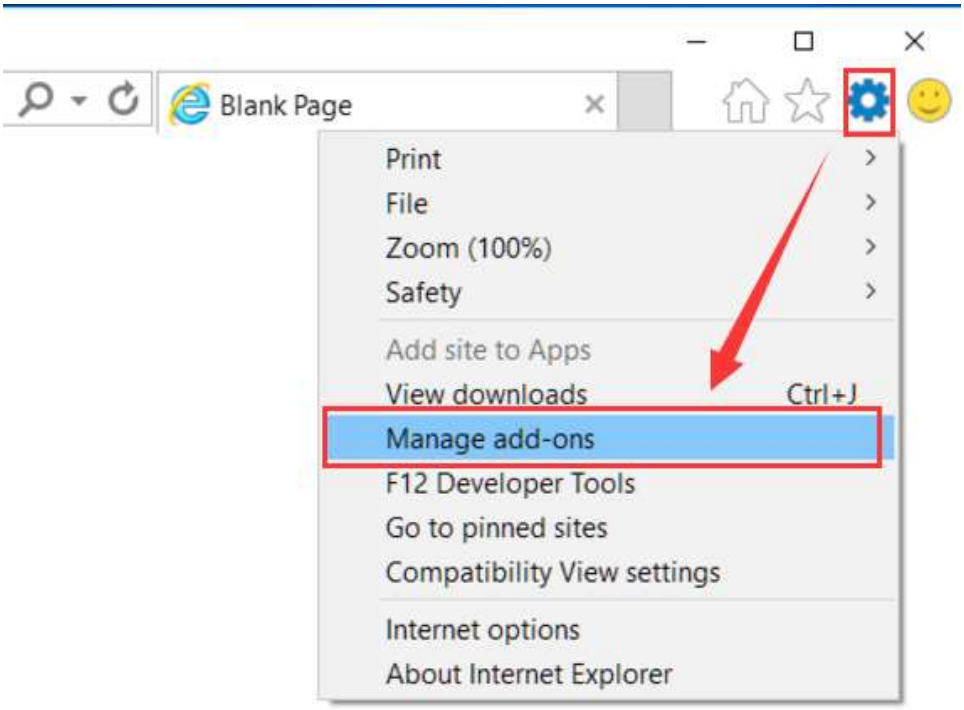


- Go to **Settings** option ➡ tap on **View Advance Settings.** Now Scroll down and turn on **"Help protect my PC from malicious sites and downloads with SmartScreen Filter"** option.

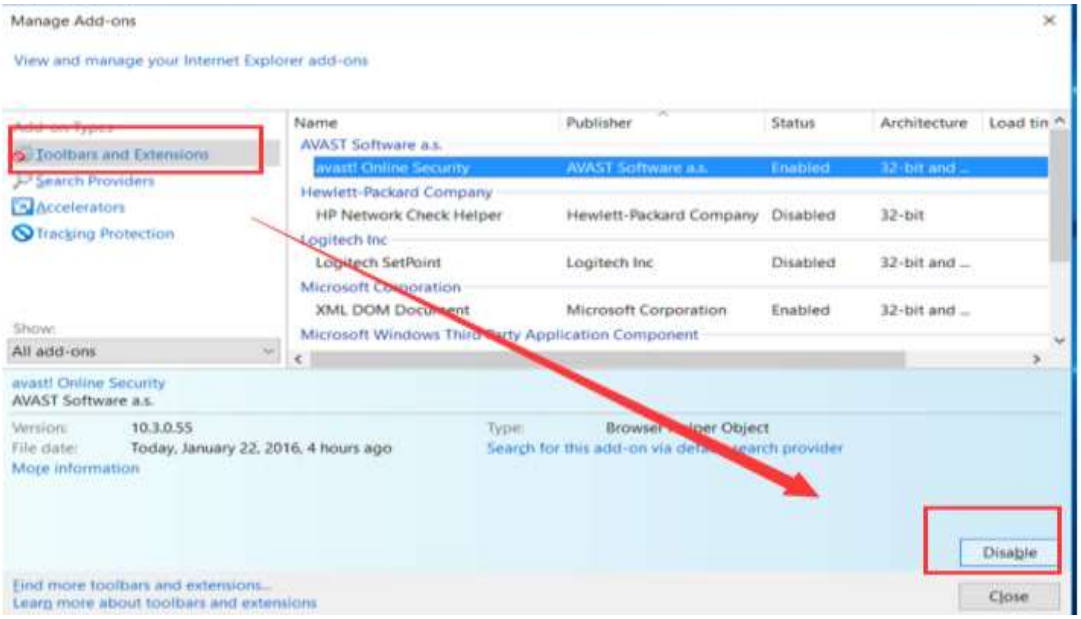


(D) : Remove Extension From Internet Explorer

- Open browser ➡ click **Tools** menu ➡ select **Manage Add-ons** option from drop down list.

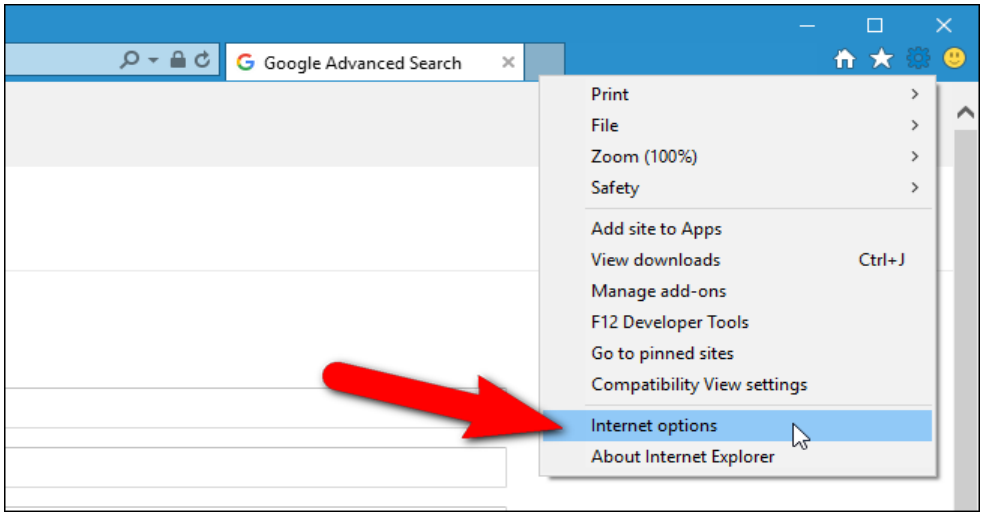


- Go to **Toolbar and Extensions** from left panel ➡ Now select Browser Hijacker and click disable tab to delete this very malicious extension completely from your system.

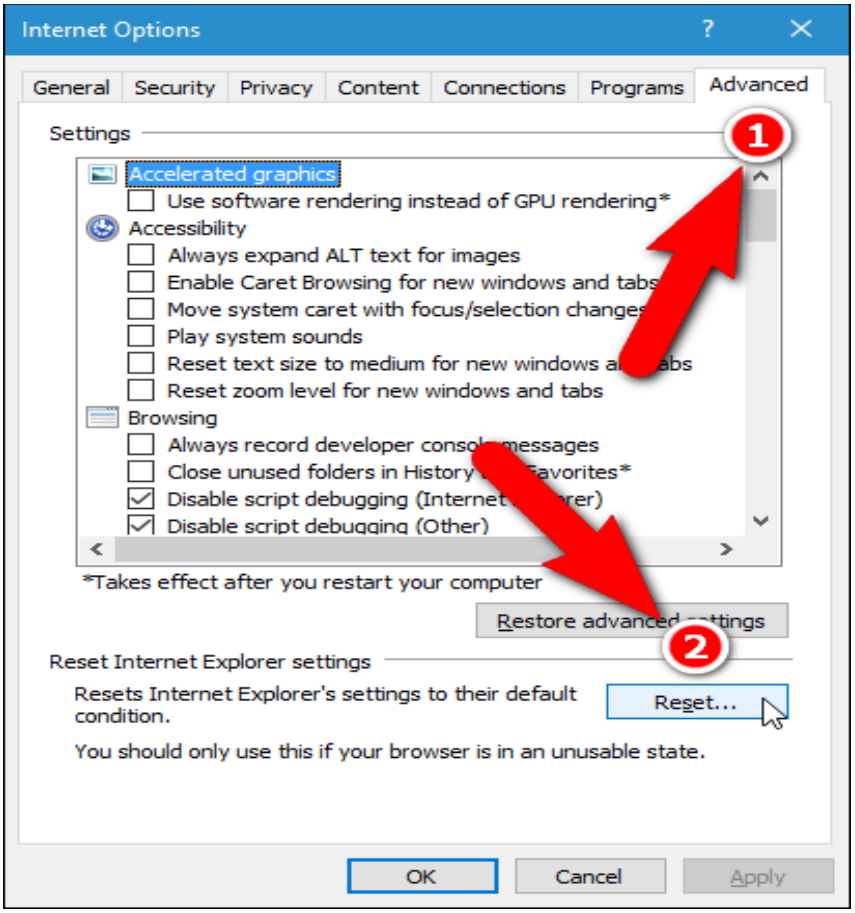


Reset Internet Explorer Setting

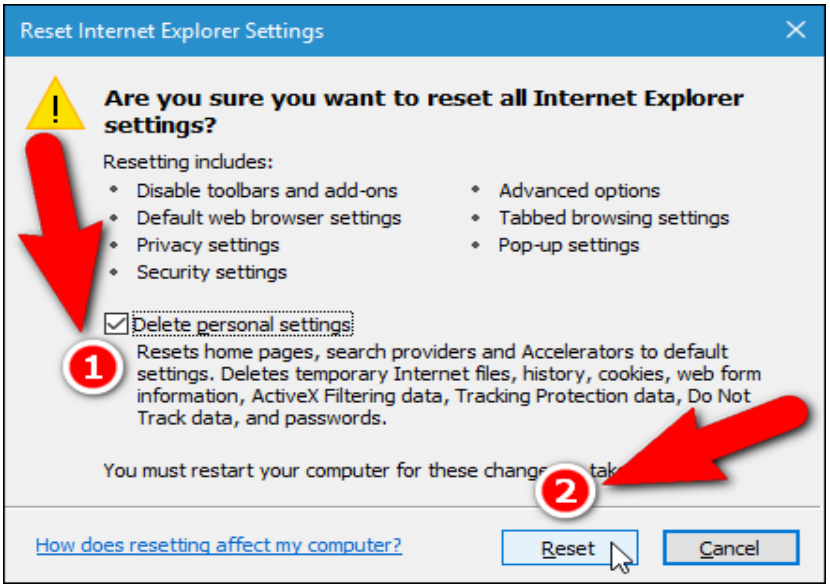
- Open **Internet Explorer** ➡ Click on **"Tools"** menu ➡ select **"Internet option"** from drop down list.



- Choose **"Advanced tab"** and hit **"Reset"** button.

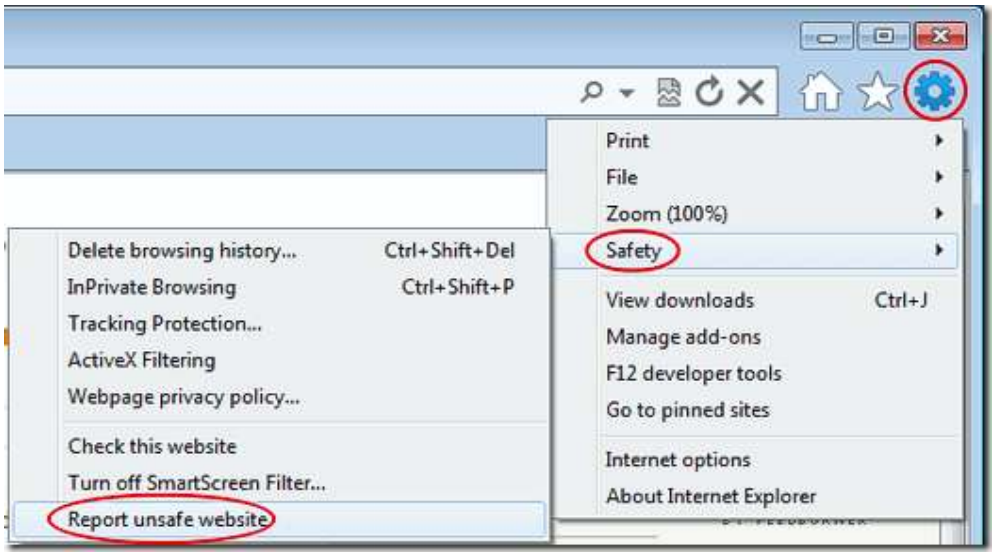


- Check out **“Delete personal settings”** check box and click on **“Reset”** button.



Enable SmartScreen Filter in Internet Explorer

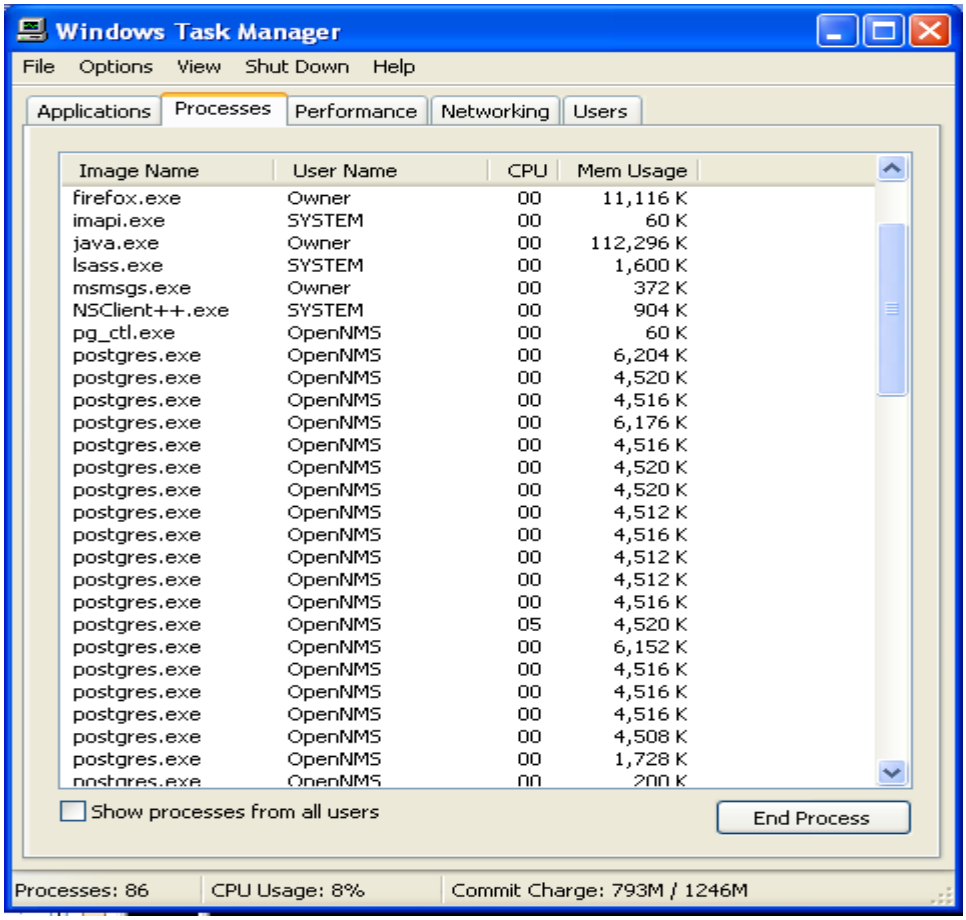
Open **Internet Explorer** ➡ Select the **Safety** option from upper menu list ➡ click on **Report Unsafe website** option to enable safe browsing.



Part 3 :- Kill Browser Hijacker Related Process Via Windows Task Manger.

- Press **Ctrl+Alt+Del** button cumulatively to open **Windows Task Manager**.

- Now click on **Process** tab to see all running process in your PC.



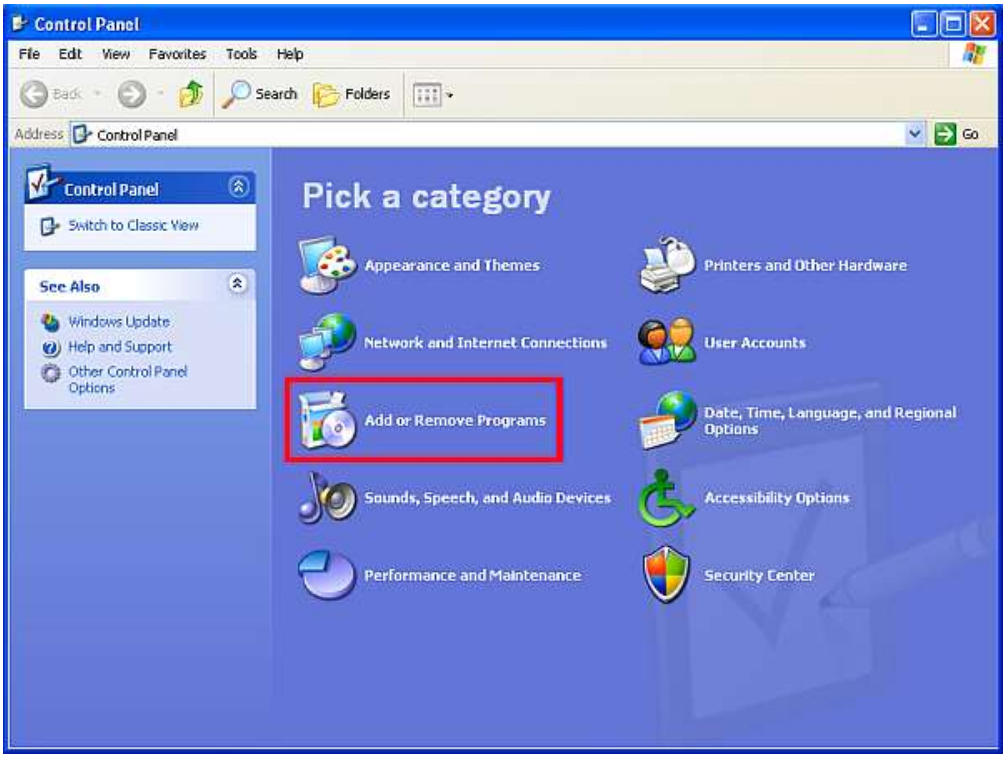
- Select all malicious process related with Browser Hijacker and click End Process option.

Part 4 :- Uninstall Browser Hijacker From Control Panel

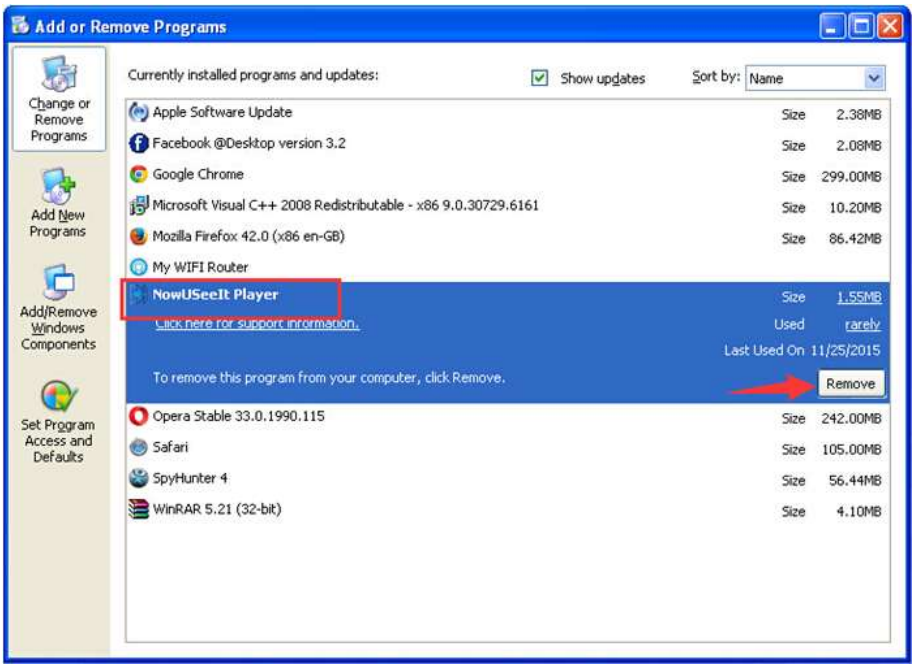
Remove From Windows XP

- Press the **Start** button and select **Control Panel** from **Start Menu**.

- Click on **Uninstall a program** option to open **Programs and Features**

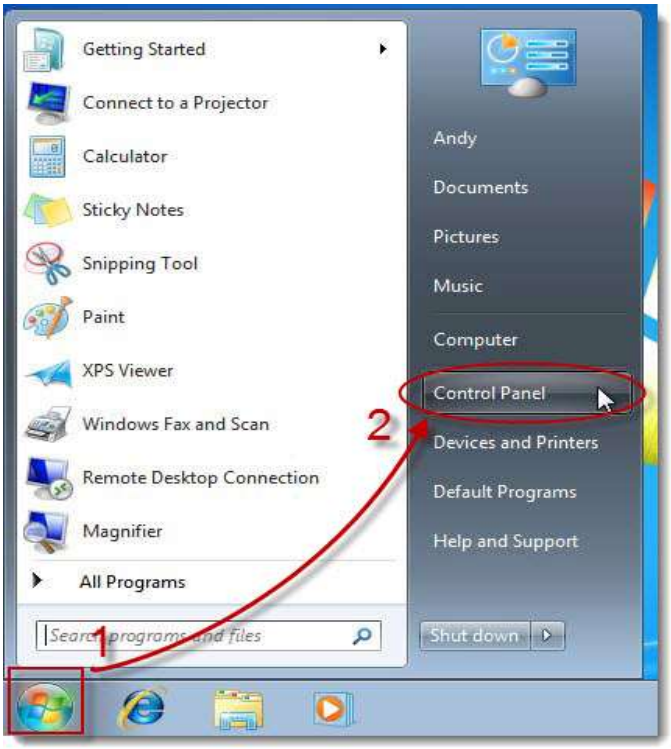


- Now find and remove all malicious application installed in your computer along with Browser Hijacker.

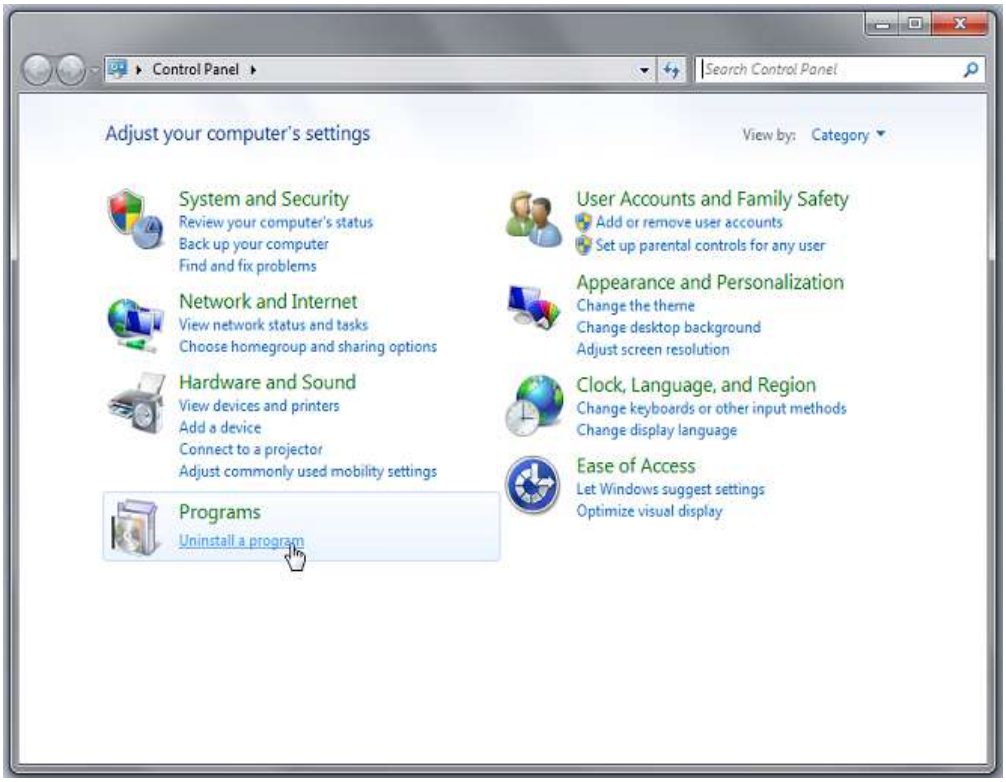


Remove From Windows 7 & Vista

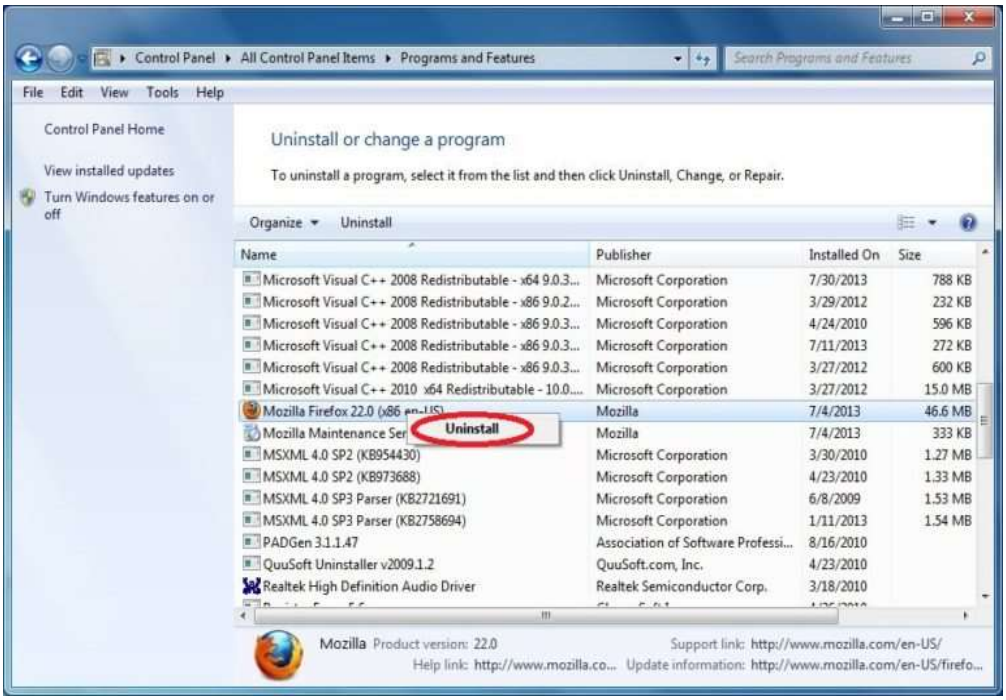
- Go to **Start Menu** and select **Control Panel** option.



- Go to **Programs** section and choose **Uninstall a program** option.



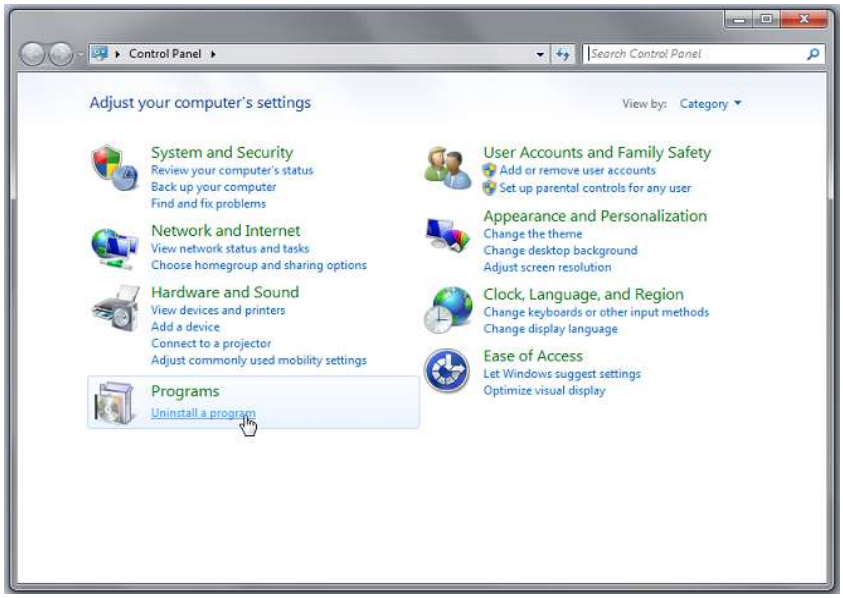
- Here, from the list of all programs select Browser Hijacker and then click **Uninstall** tab.



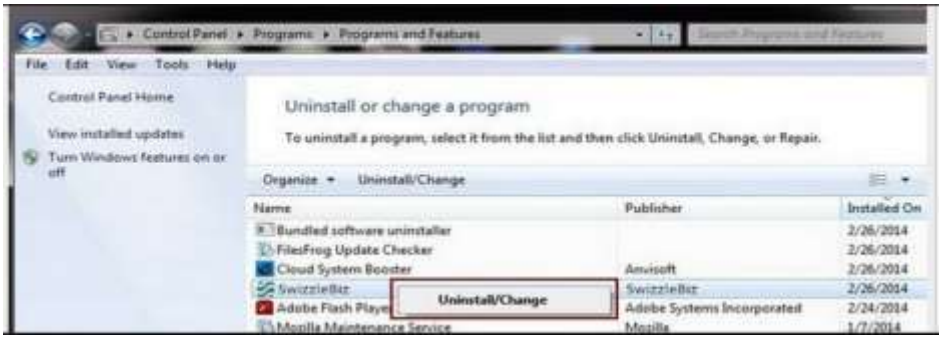
Remove From Windows 8 & 8.1

- Turn the cursor to lower-left corner of your computer screen and click **Start** button.

- Now search for **Control Panel** in the **search box** and then click **Control Panel**.

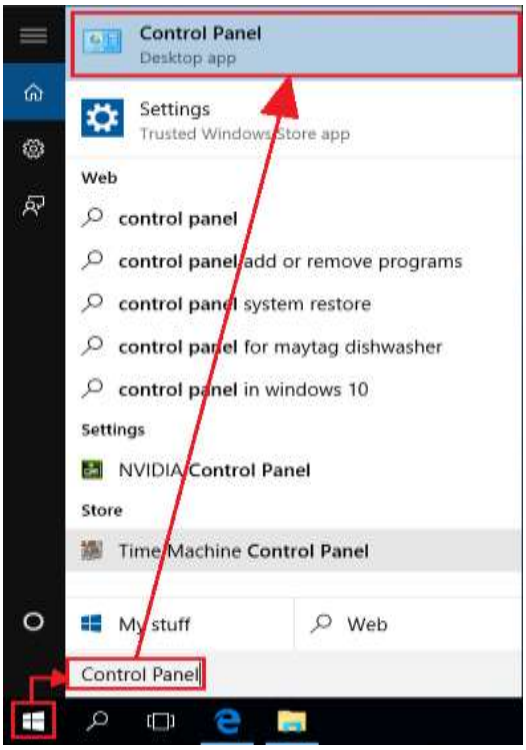


- Find out all application related with Browser Hijacker and hit Uninstall tab.

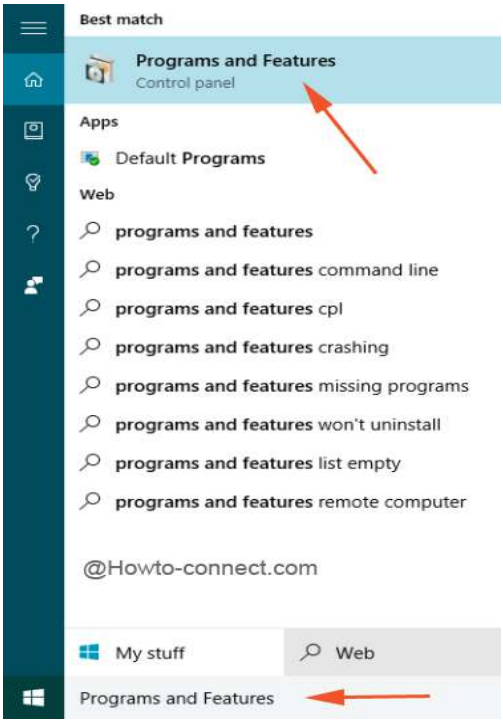


Remove From Windows 10

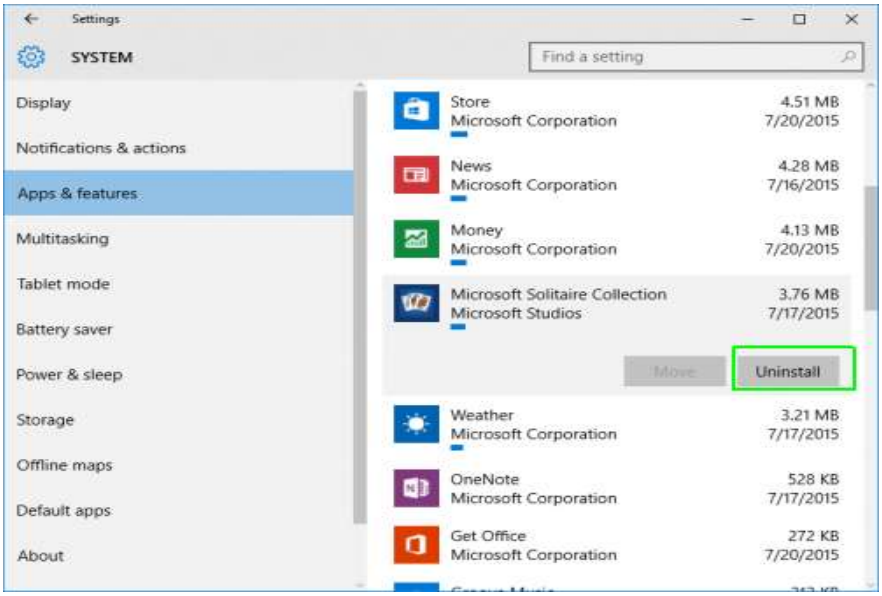
- Go to **Start** Menu and search for **Control Panel**.



- Now select **Programs and Feature** option in **Control Panel** window.



- From the list of all programs select Browser Hijacker and hit **Uninstall** tab.

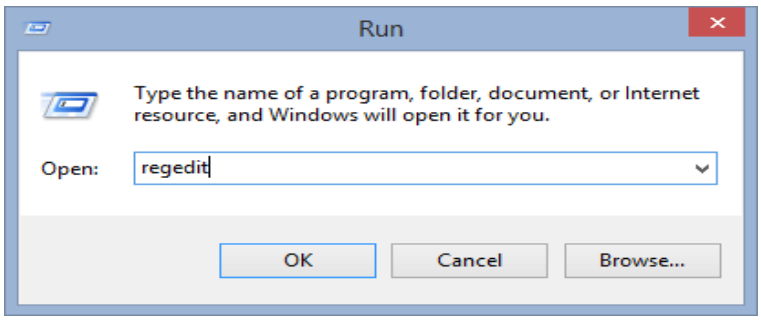


- Finally a confirmation Window will appear on your screen, click yest to confirm and **restart** PC.

Part 5 :- Remove Browser Hijacker From Registry Editor

- Press **“Windows + R”** button together on your keyboard.

- Type **“regedit”** and click on **OK** button to open **Registry Editor**.



- Find and delete all malicious registry entries created by Browser Hijacker virus.

Registry Keys Created by Browser Hijacker

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msmpeng.exe "Debugger" = 'svchost.exe'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msseces.exe "Debugger" = 'svchost.exe'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Browser Hijacker

HKEY_LOCAL_MACHINE\SOFTWARE

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings "WarnOnHTTPSToHTTPRedirect" = '0'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings "WarnOnHTTPSToHTTPRedirect" = '0'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore "DisableSR " = '1'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ekrn.exe "Debugger" = 'svchost.exe'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msascui.exe "Debugger" = 'svchost.exe'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "3948550101?

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "xas"

HKEY_CURRENT_USER\Software\Browser Hijacker

Tips For Preventing Browser Hijacker And Other Malware In Future

Once you remove this infection completely from your PC, you must beware of these kind of attacks. As it is said that prevention is better than cure, so you are advised to avoid such type of malware intrusion in future. Here are some tips given below that can help you to stay safe online.

- Never download free software or updates from untrusted websites.
- Do not click on misleading and fake advertisement.
- Try to avoid visiting malicious or pornographic websites.
- Always keep your system and program updated.
- Download update only from authentic and official websites.
- Always use a powerful anti-virus and malware removal program.
- Regularly Scan your PC for hidden threats, malware and viruses.
- Always scan external USB drives before doing file transfer.
- Choose custom installation process to avoid bundled malware and PUP.
- Do not open spam emails from unknown sender that carry any attachments.
- Scan all the spam email attachment before opening it.