How To Remove Trojan Virus From Windows OS?

Detailed instructions To Remove Trojan Virus From Windows OS.

- Step 1 : Manually Killing the malicious processes, disabling suspicious programs and then removing the remaining virus and its traces by scanning.
  - Open task manager and kill the .exe process for the virus.
  - Disable any suspicious program from startup.
  - Boot the PC in safe mode and scan for the Trojan virus.
- Step 2: Remove Trojan virus using System Restore Procedure.
- Step 3: Reboot your computer to Safe Mode with Command Prompt.
- Step 4: Restore your system files and settings.
- Step 5: Download effective antivirus program and scan your computer to ensure successful removal of Trojan threat.

Step 1. Manually Killing Malicious Processes

1.1 Open task manager and kill the .exe process for the virus

Although it is difficult to trace a trojan threat manually, you can a little about trojans and its activities then you can locate them within the task manager windows. You can look for any suspicious processes running within the background and end the tasks. After deleting the tasks you need to manually delete the suspicious files from the location.

Follow any of the ways to open task manager on your Windows OS:

- Click on the “Start” menu, select Run(win+R), and type “taskmgr”.
- Type “task manager” within the search box on your taskbar.
- Press Ctrl + Alt + Delete and select “Task Manager” from the option.
- Press Ctrl + Shift + Esc.
- Right-click the taskbar and select Task Manager from the menu.

Now once the task manager window opens, perform these steps:

1. Under the process tab, check for the suspicious program still running;
2. If you find it, right click on the name and select “Open file location”;
3. Then click on “End Task”;
4. Now go to the file location window opened and select the program, then right click and choose “delete”.
5. Don’t forget to Empty the Recycle Bin after that because such programs can revive themselves from recycle bin folder.

Step 1.1 Disable Suspicious Programs From Startup

Once you have done with the registry cleaning, now you need to exit from safe mode. To exit, click on Start → Power → Restart

It is very important to know which programs or applications are set to auto-launch when the system boots. If any suspicious program is launching after every system restart, then it will not allow you to remove it completely from the infected system. And there is very much chances that it will again repair its files and be active on your system.

So, here is the step which you need to follow for disabling the suspicious programs from auto-launch.

1. Press Windows key + S that will open the search box. Within the search field type "msconfig" that will launch "System Configuration" window. Check the search results and click when it appears. When it appears in the search results, click on it to open the application.
2. Once the window opens, click on the Startup tab to see the list of programs which are set to auto-launch with the computer boot. The list is displayed on the startup tab itself for the windows 7/xp and vista. For newer versions like Windows 8 and 10 users will be asked to open the Task Manager to see the list. Go through it to follow the next steps.
3. Now browse the list to locate anything suspicious that appears to you as adware. If you are not sure of any program then search it on the web if it is from any company or not. If you find it illegitimate then, you need to disable them from the startup. To disable a program, if you are on Windows 7/xp/vista then, uncheck the box next to the program name. For Windows 8 or 10- click on the program, then click "Disable" button appearing at the bottom of the window).

Step 1.2 Safe Mode with Networking:

First of all, you need to remove all external media like any USBs, CDs and flash drives and so.

There are three boot options available:

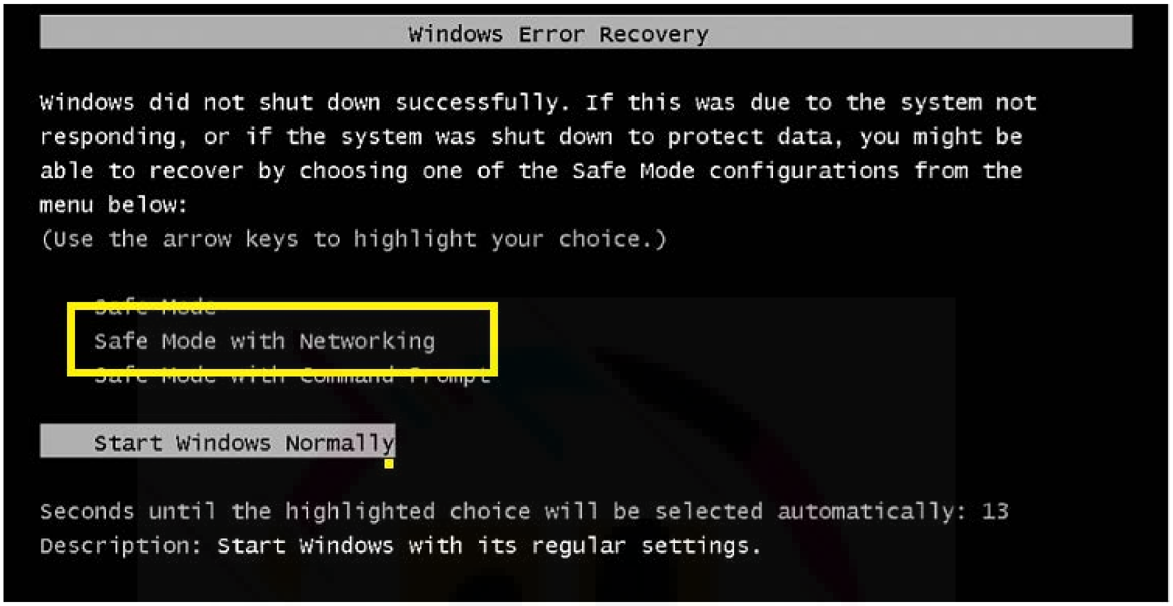
- Safe Mode – This boot option starts the Windows with only necessary processes without the networking. This is usually the default boot mode when you don't need the internet connection and unnecessary programs.
- Safe Mode with Networking – This boot option will start the windows with the same necessary processes but along with networking functions. So you need to choose this option when you need an internet connection or access your local network while troubleshooting windows.
- Safe Mode with Command Prompt – This option of safe mode starts with the Command prompt interface instead of normal windows desktop interface. This safe mode option also loads of minimum processes and can be used when safe mode boot option does not work well for you.

Windows 7/Vista/XP - Safe Mode

1. Click on the Start menu, then on click the arrow next to "Shut Down." Select Restart. (Just as you normally Restart your PC).
2. Once the computer screen is powered on, immediately start tapping "F8" key till you see "Advanced Boot Options" screen. if you don't enter to the boot screen, then restart the

process again and press F8 while the PC is restarting.

3. Here, you need to choose Safe Mode with Networking option and press “enter” key to troubleshooting windows. As later on, you need to access the internet.
4. Once you choose the Safe Mode with Networking option wait for the system to load necessary system files.



```
                        Windows Error Recovery

Windows did not shut down successfully. If this was due to the system not
responding, or if the system was shut down to protect data, you might be
able to recover by choosing one of the Safe Mode configurations from the
menu below:
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Start Windows Normally

Seconds until the highlighted choice will be selected automatically: 13
Description: Start Windows with its regular settings.
```

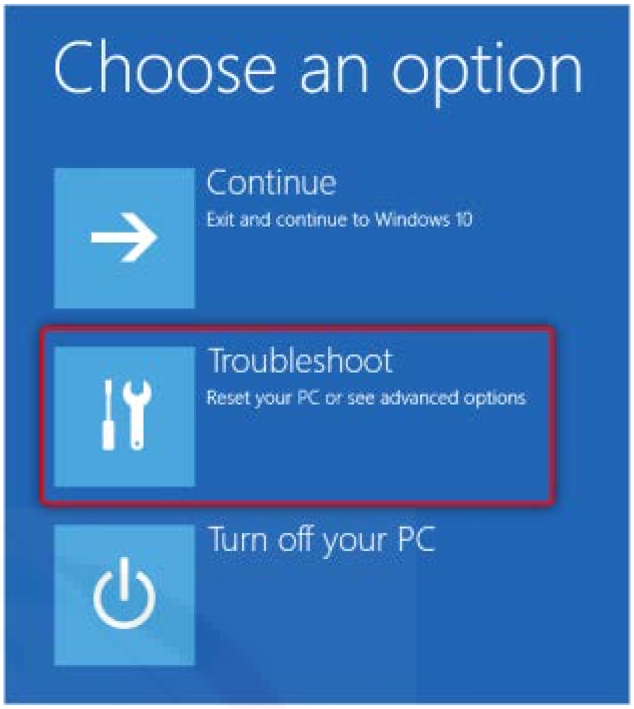
Open In Safe Mode Win 7

5. And you will now see the login screen. Now log in with your Administrator Account.

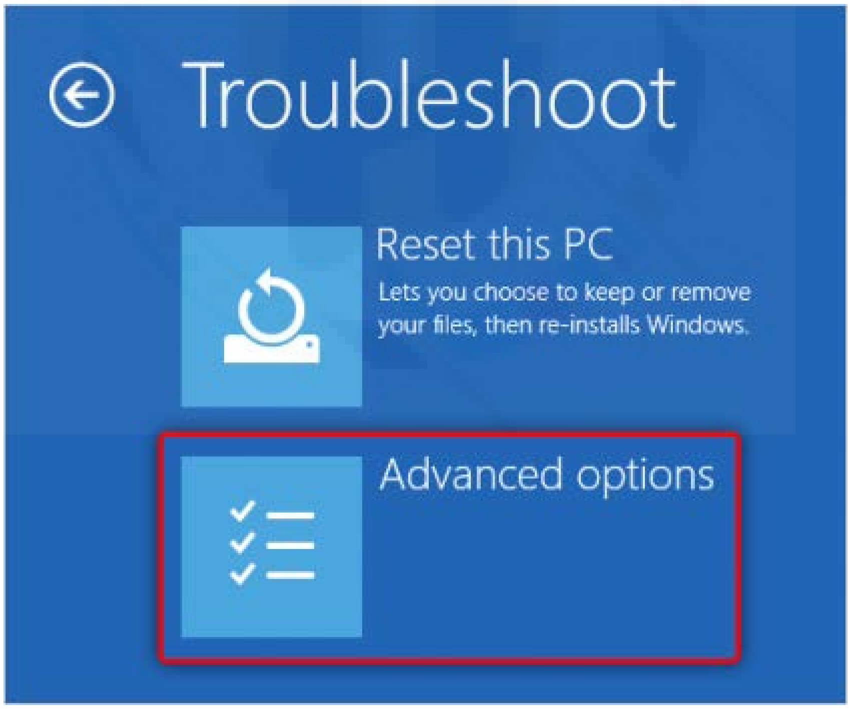
NOTE: To get back to your normal windows configuration, you need to repeat steps 1-3 and select Start Windows Normally.

Windows 10, 8/8.1 - Safe Mode- Safe Mode

1. For Windows 10: Click Start → Power and then hold the Shift key on your keyboard and click Restart.
2. For Windows 8/8.1: Press the “Windows key + C“, and then click “Settings“. Click “Power“, hold down the Shift key on your keyboard and then click “Restart“.
3. From here steps are same for Windows 10 and 8.
4. Click Troubleshoot.
5. Click Advanced options.

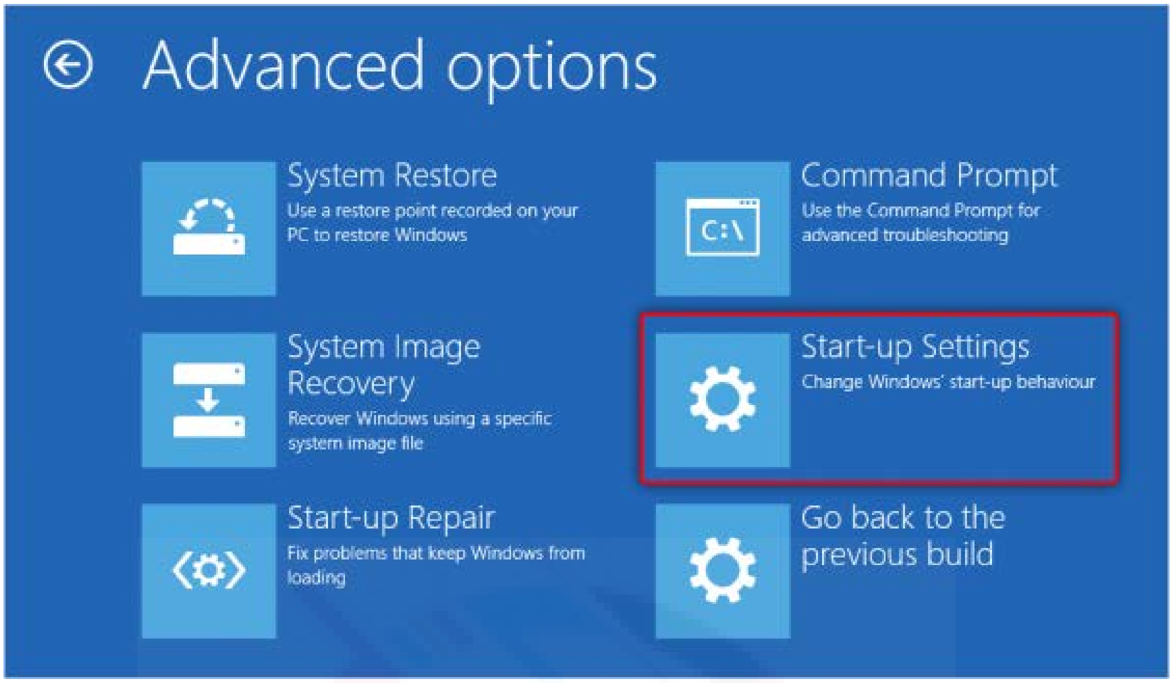

Choose an option
Continue
Exit and continue to Windows 10
Troubleshoot
Reset your PC or see advanced options
Turn off your PC

Choose Troubleshoot


Troubleshoot
Reset this PC
Lets you choose to keep or remove your files, then re-installs Windows.
Advanced options

Choose Advanced Options

6. Click Startup Settings.



Advanced options

System Restore
Use a restore point recorded on your PC to restore Windows

Command Prompt
Use the Command Prompt for advanced troubleshooting

System Image Recovery
Recover Windows using a specific system image file

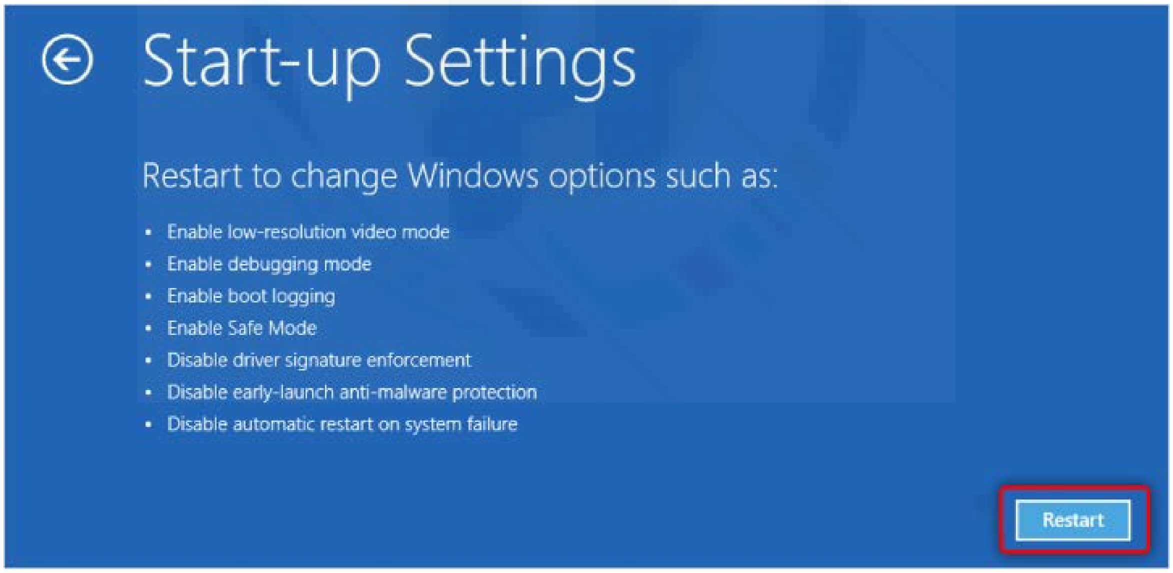
Start-up Settings
Change Windows' start-up behaviour

Start-up Repair
Fix problems that keep Windows from loading

Go back to the previous build

Choose Start-up Setting

7. Click Restart.



Start-up Settings

Restart to change Windows options such as:

- Enable low-resolution video mode
- Enable debugging mode
- Enable boot logging
- Enable Safe Mode
- Disable driver signature enforcement
- Disable early-launch anti-malware protection
- Disable automatic restart on system failure

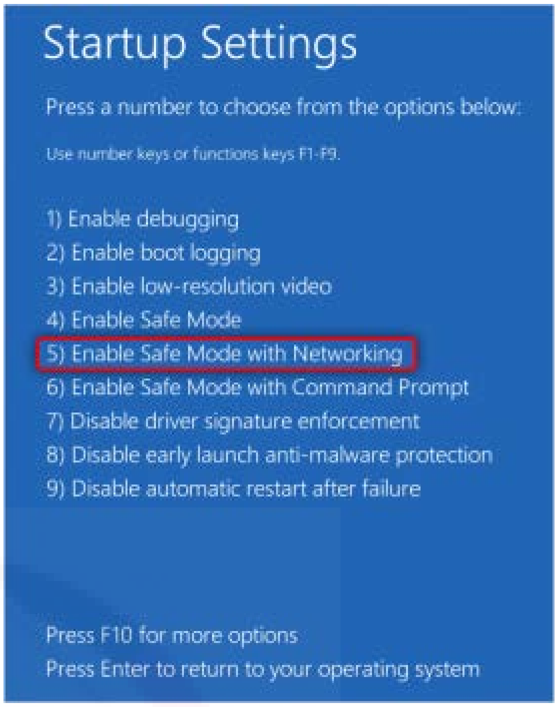
Press Restart

8. After your computer restarts, press 5 or F5 on your keyboard to select Safe Mode with Networking.
9. Enter your Administrative username and password to start Windows in Safe Mode with Networking.

NOTE: To get back to normal Windows configuration you need to Click Start → Power and then click Restart.

Once you are on safe mode with networking, start your browser and check for the any suspicious program that might be hiding in the form of rogue extensions, fake plug-ins and infected add-ons from the browsers. These browser helper objects may take the form of any malware and does annoying activities. Do for all the browsers installed on your computer one by one.

NOTE: If your browser is working fine then you can skip this step and carry out the removal process further.



Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

1) Enable debugging
2) Enable boot logging
3) Enable low-resolution video
4) Enable Safe Mode
5) Enable Safe Mode with Networking
6) Enable Safe Mode with Command Prompt
7) Disable driver signature enforcement
8) Disable early launch anti-malware protection
9) Disable automatic restart after failure

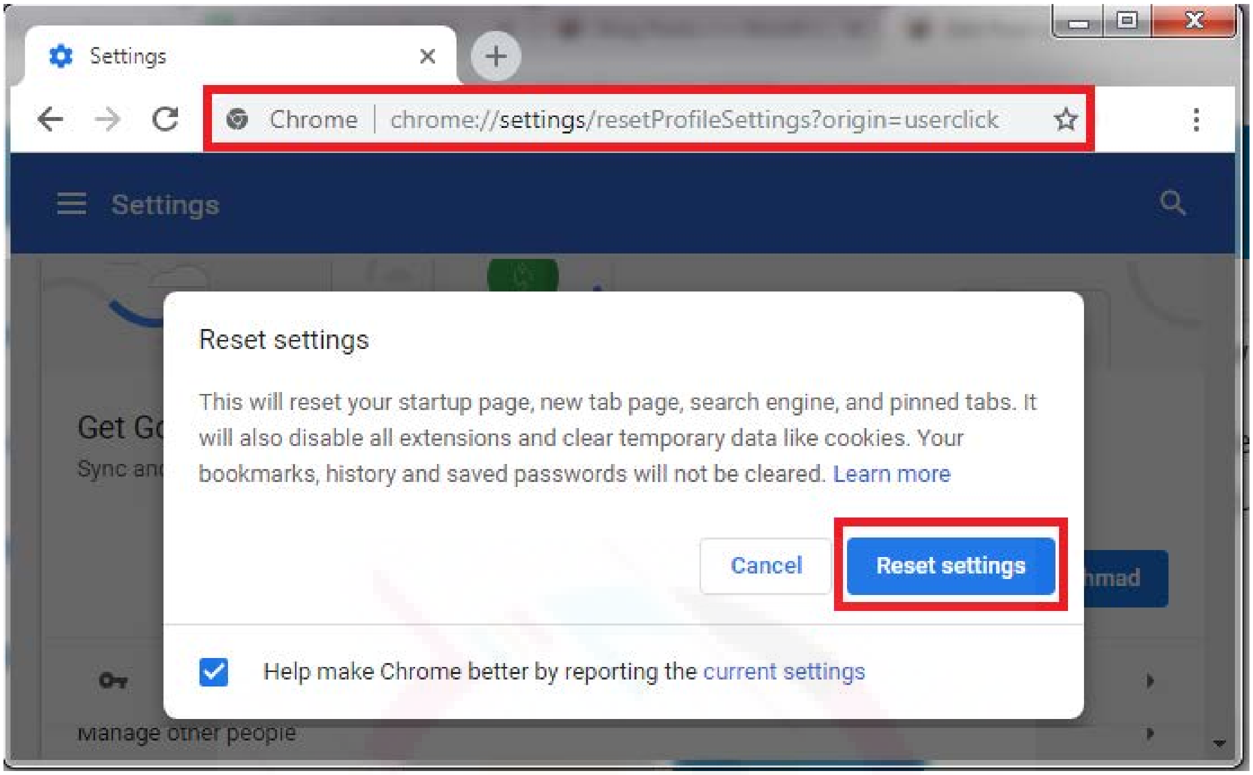
Press F10 for more options
Press Enter to return to your operating system

Choose Safe Mode With Networking

Reset Google Chrome

Browser resetting can be done anytime if you are noticing any unwanted modifications to the preferred browser settings of yours. Resetting will not remove your saved bookmarks and passwords. However, the new tabs, browsing history, search engine, and extensions are cleared and set to default. To reset your chrome follow the quick steps:

Method 1: This is the URL for the reset chrome browser “chrome://settings/resetProfileSettings?origin=userclick”, just copy the URL and paste it into the address bar.



Reset settings

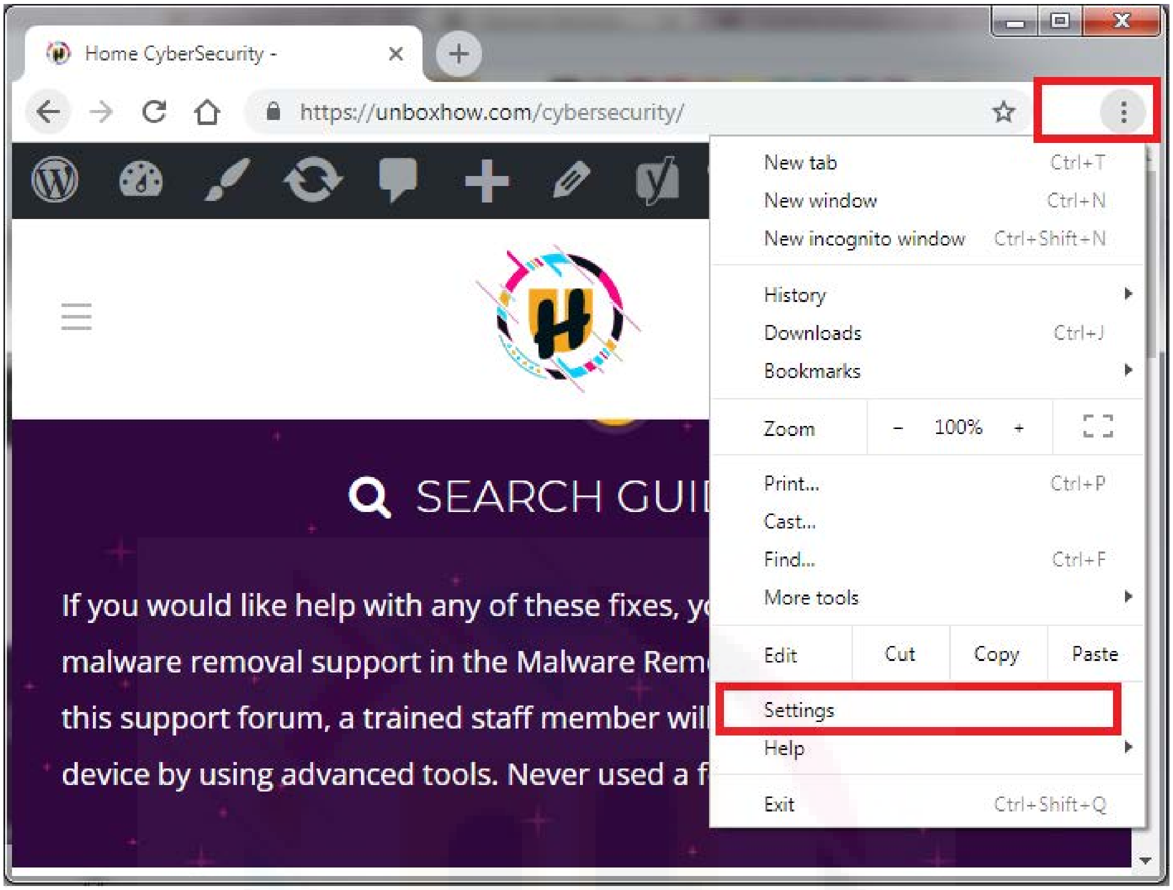
This will reset your startup page, new tab page, search engine, and pinned tabs. It will also disable all extensions and clear temporary data like cookies. Your bookmarks, history and saved passwords will not be cleared. Learn more

☑ Help make Chrome better by reporting the current settings

Reset Chrome

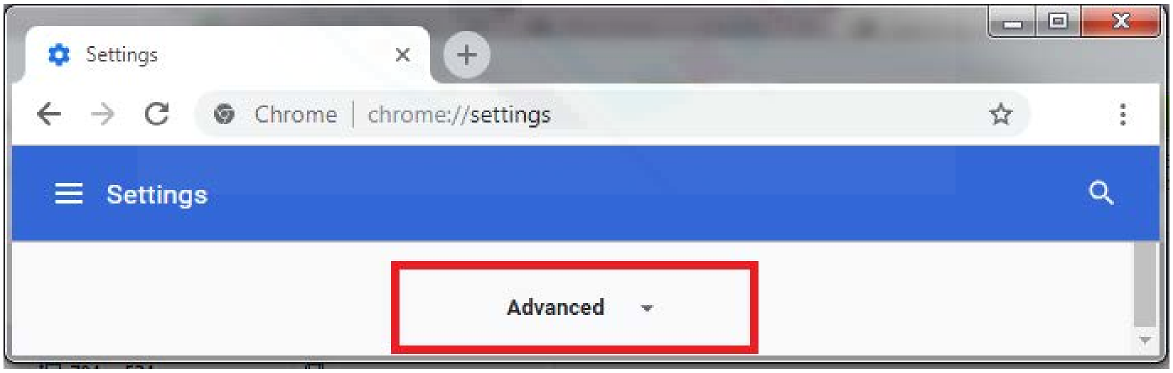
Method 2:

1. Click on "Chrome's Menu" then choose "Settings";


Home CyberSecurity -
https://unboxhow.com/cybersecurity/
New tab Ctrl+T
New window Ctrl+N
New incognito window Ctrl+Shift+N
History
Downloads Ctrl+J
Bookmarks
Zoom - 100% +
Print... Ctrl+P
Cast...
Find... Ctrl+F
More tools
Edit Cut Copy Paste
Settings
Help
Exit Ctrl+Shift+Q
SEARCH GUI
If you would like help with any of these fixes, yo
malware removal support in the Malware Rem
this support forum, a trained staff member will
device by using advanced tools. Never used a f

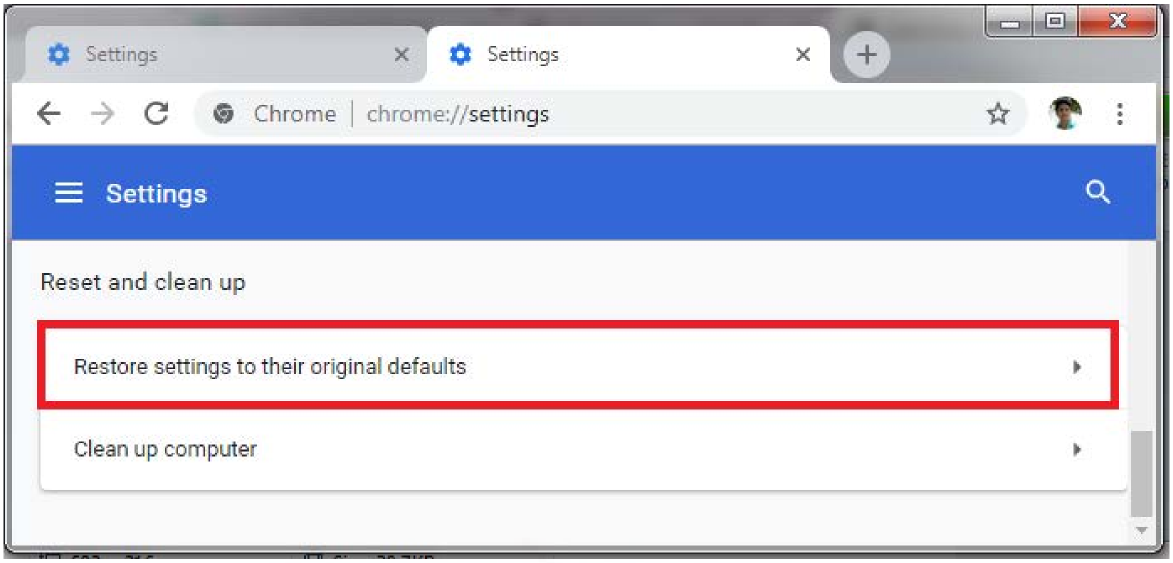
Reset Browser Chrome 1

2. A settings window will appear, scroll to the bottom and, click "Advanced";



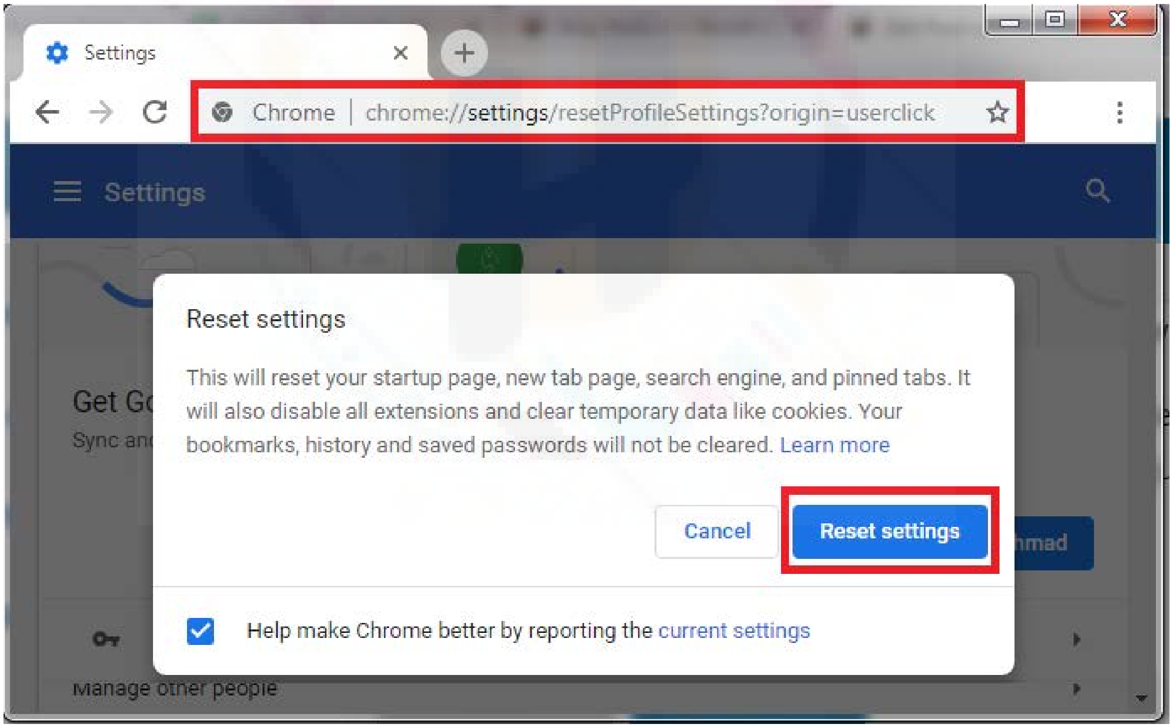
Reset Browser Chrome 2

3. Now, scroll down to the "Reset and cleanup," section;


Settings
Settings
Chrome | chrome://settings
Settings
Reset and clean up
Restore settings to their original defaults
Clean up computer

Reset Browser Chrome 3

4. Click on “Reset Settings” → Reset Settings to confirm the reset.


Settings
Chrome | chrome://settings/resetProfileSettings?origin=userclick
Settings
Get Go
Sync an
hmad
Manage other people

Reset settings

This will reset your startup page, new tab page, search engine, and pinned tabs. It will also disable all extensions and clear temporary data like cookies. Your bookmarks, history and saved passwords will not be cleared. Learn more

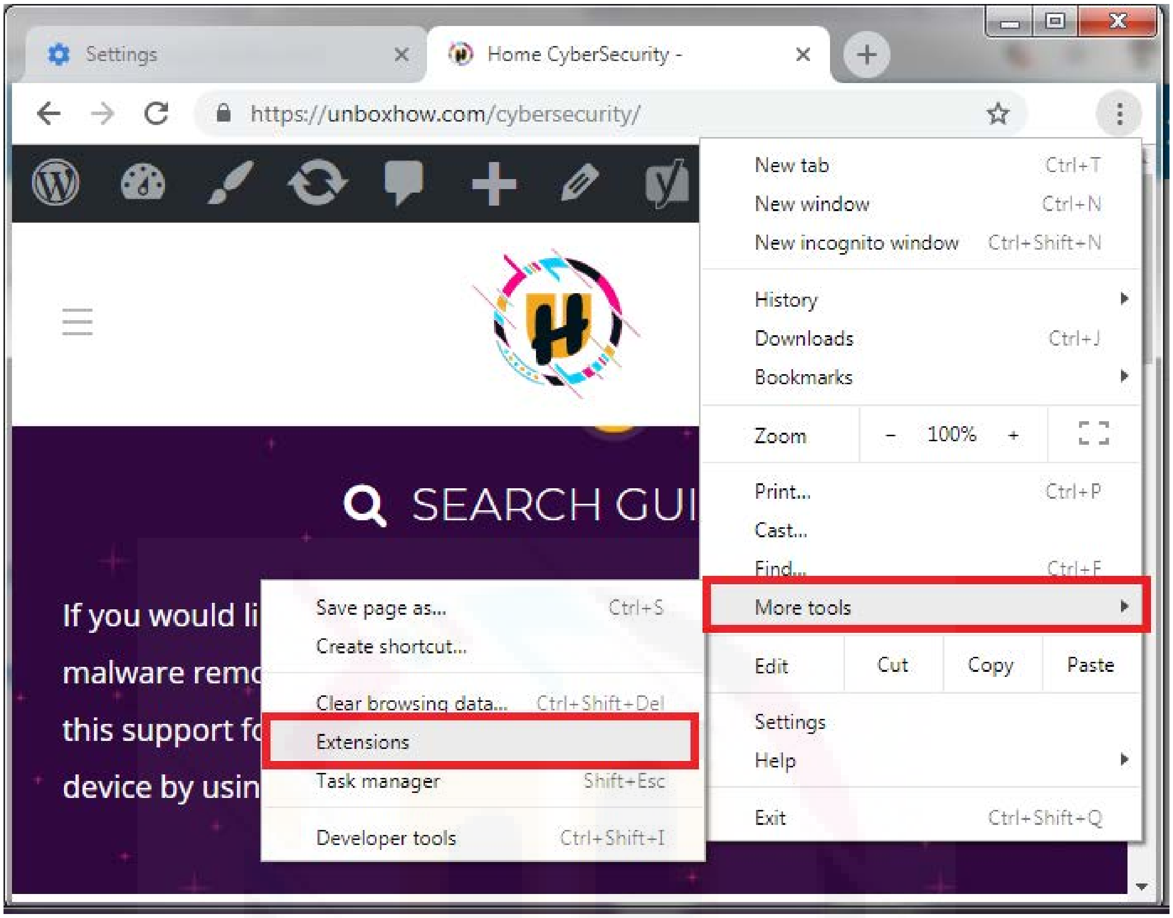
☑ Help make Chrome better by reporting the current settings

Reset Browser Chrome 4

Removing unwanted extensions

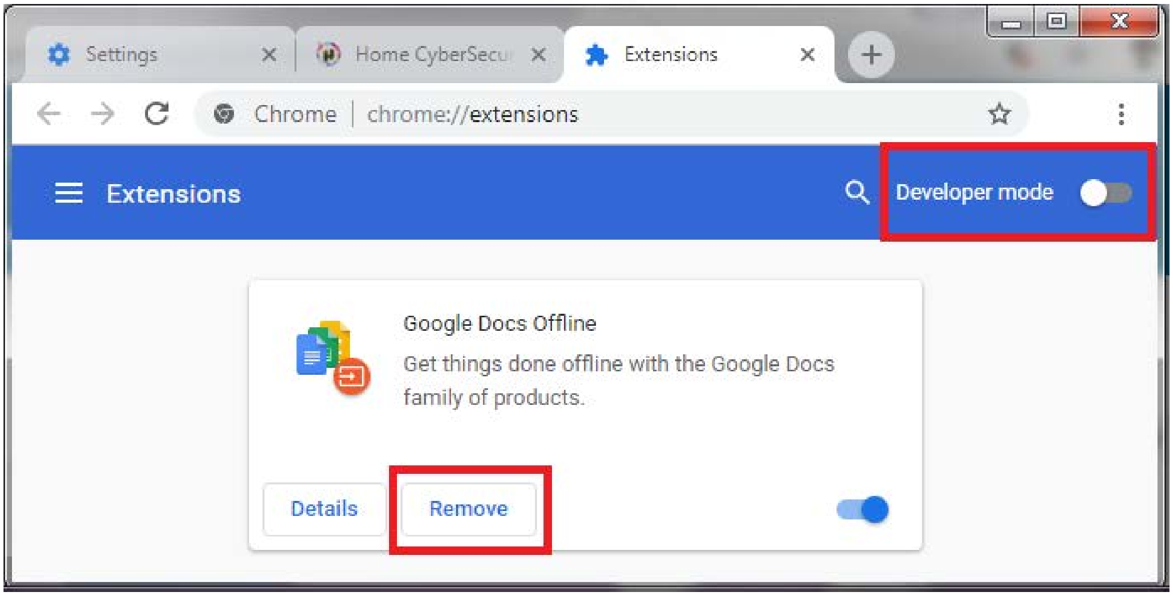
Steps by slightly differ due to browser versions, to avoid any clash simply copy this URL “chrome://extensions/”, paste it into the search bar and hit enter.

1. Click the Chrome menu appearing on the top right corner of the browser as three vertical dots;
2. Select “More Tools” and the Click “Extensions”.



Remove Chrome Extensions 1

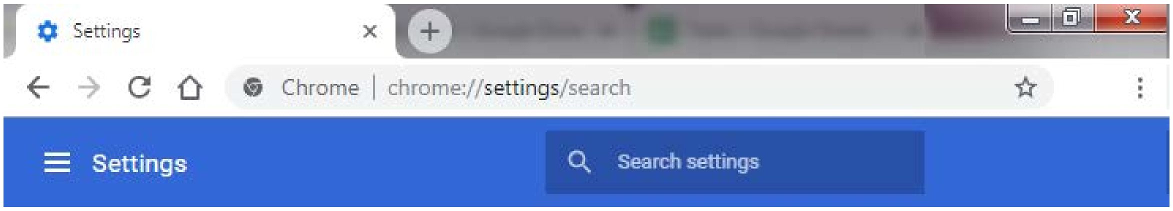
3. Once the extension page appears, look for any suspicious extension that you may have to choose to install.
4. Click on the trash icon or “Remove” button.
5. Also, disable the Developer Mode if enabled.


Settings
Home CyberSecu
Extensions
Chrome | chrome://extensions
Extensions
Developer mode
Google Docs Offline
Get things done offline with the Google Docs family of products.
Details
Remove

Remove Chrome Extensions 2

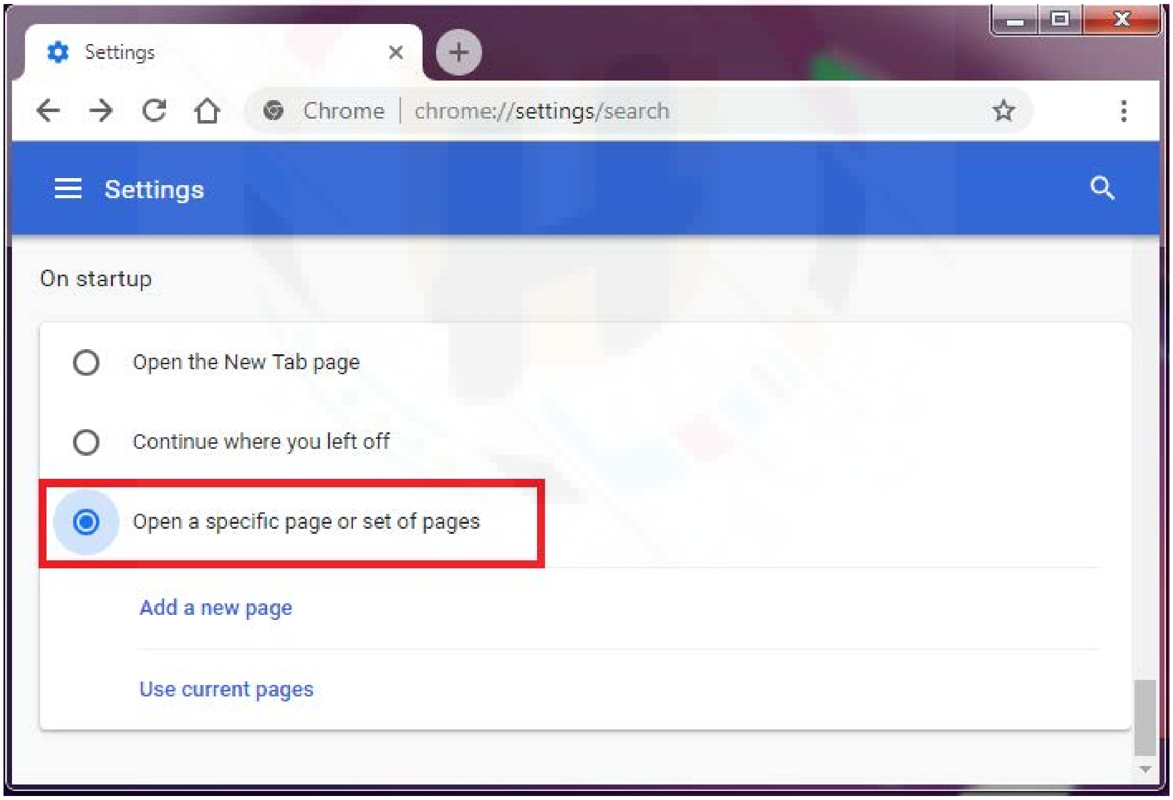
Check for existing start page, search engines, and other defaul ts

1. Again from the menu click on settings and go to Set page (for older version), in the newer version on the left menu choose "Search engine".
   Or simply copy, paste this URL "chrome://settings/search" on browser address bar and hit "enter".)



Reset Chrome Browser Search Engine 1

2. Scroll down to find the 'On startup' section where you will get 'Open a specific page or set of pages' and then click on Set pages(older version) .



On startup

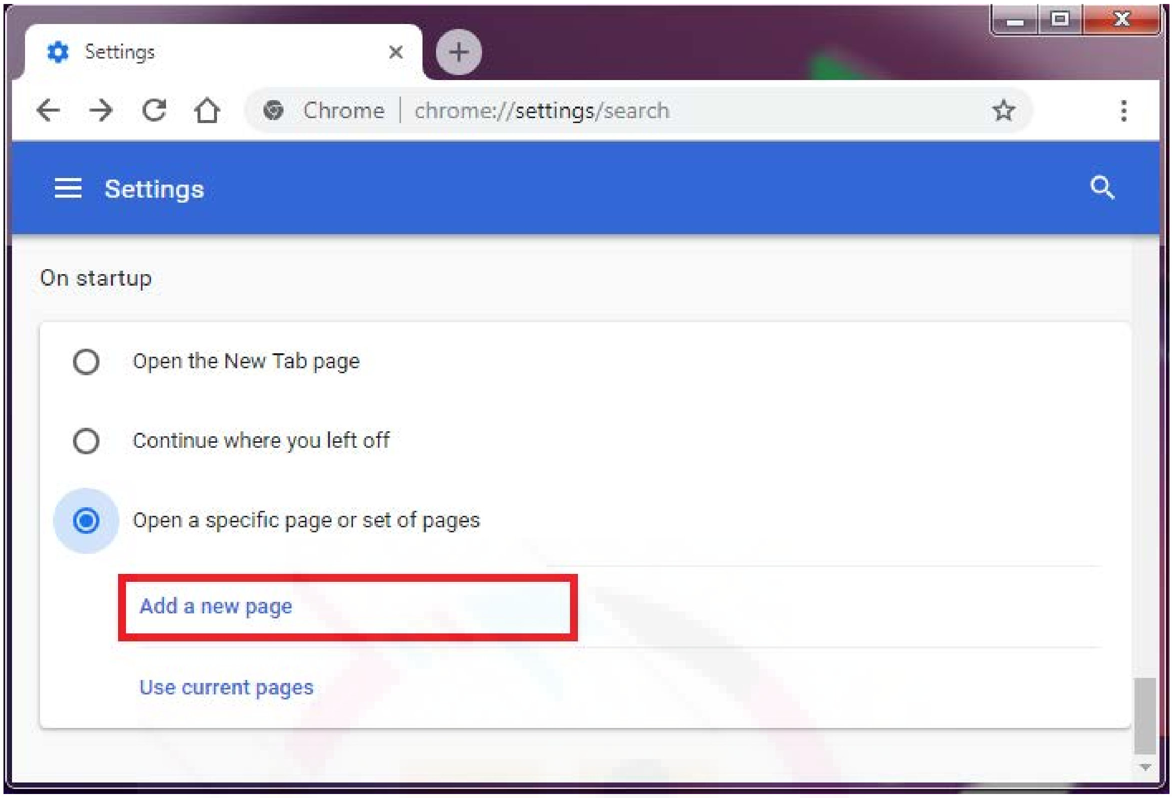
○ Open the New Tab page

○ Continue where you left off

● Open a specific page or set of pages

Reset Chrome Browser Search Engine 2

3. Now check the URLs listed there and click on the X button to remove any unwanted/hijacked start-page. For new version click on the three vertical dots and click on "Remove".
4. After all the infected or hijacker start pages are removed, then add a new start-page by clicking on "Add a new page" and type "http://www.google.com" to set Google as your default startup page.



On startup

○ Open the New Tab page

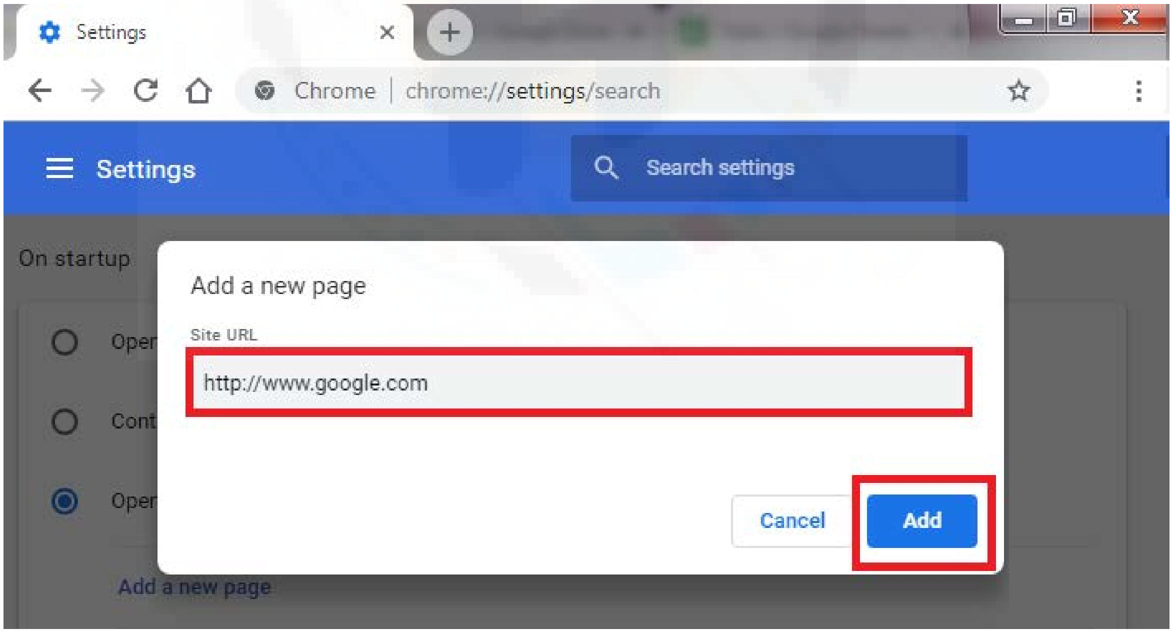
○ Continue where you left off

● Open a specific page or set of pages

Add a new page

Use current pages

Reset Chrome Browser Search Engine 4

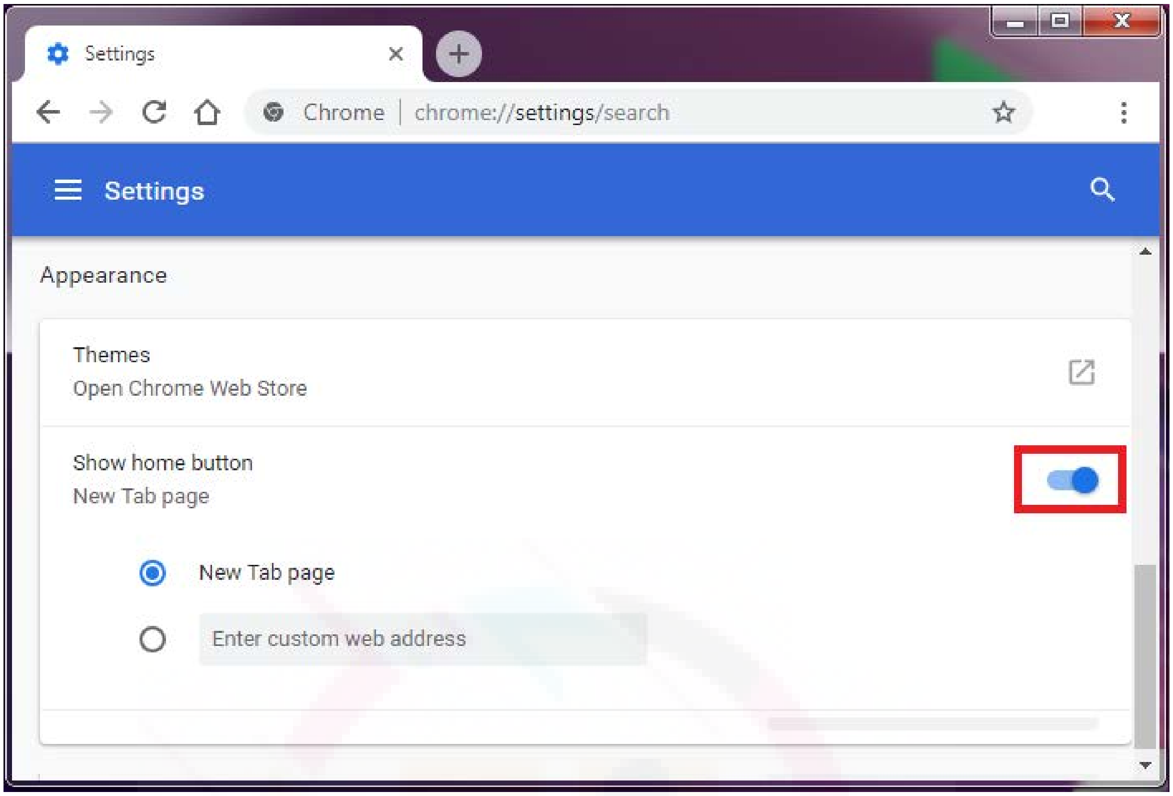


Add a new page

Site URL: http://www.google.com

Reset Chrome Browser Search Engine 5

5. Now scroll above to the Appearance section and click on the Checkmark on “Show Home Button” for an older version and click on the radio button next to the default URL added above “http://www.google.com” (for the new version)and click Change.



Appearance

Themes
Open Chrome Web Store

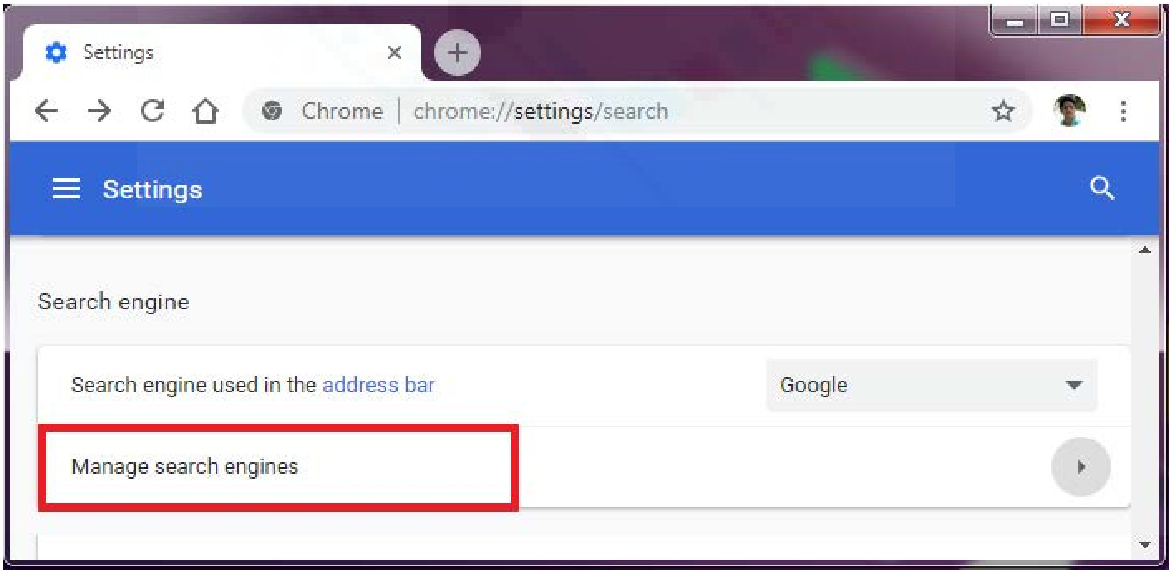
Show home button
New Tab page

● New Tab page

○ Enter custom web address

Reset Chrome Browser Search Engine 6

6. Next, you need to manage the search engine settings, Scroll down to the 'Search' or "Search engine" section(depends on the browser version) and click on the option Manage search engines;



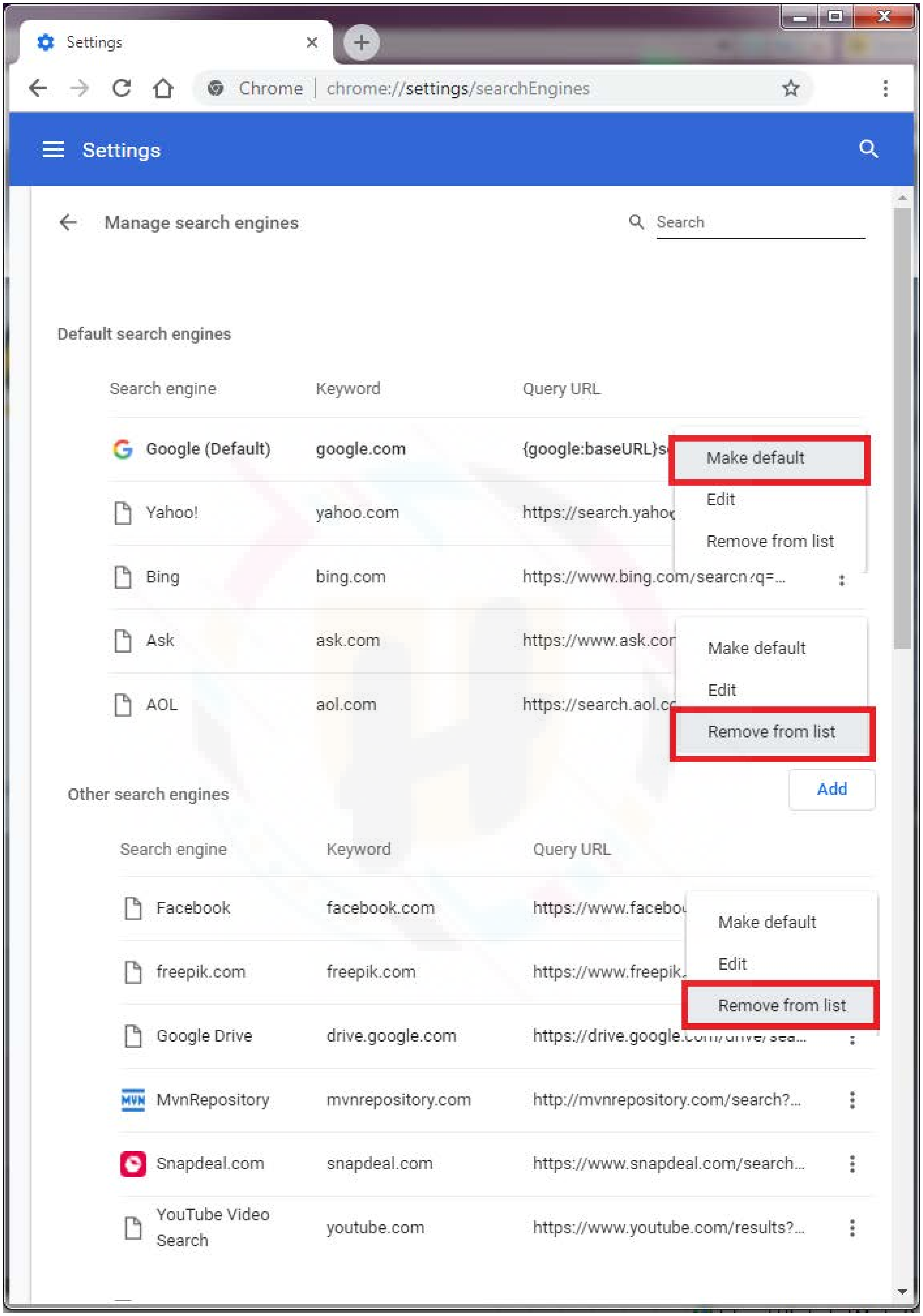
Search engine

Search engine used in the address bar: Google

Manage search engines

Reset Chrome Browser Search Engine 7

7. Select your preferred search engine from the list and(mark as default) if remove the unwanted ones by clicking on "X" button or three vertical dots and click remove.



Default search engines

Search engine	Keyword	Query URL
Google (Default)	google.com	{google:baseURL}s
Yahoo!	yahoo.com	https://search.yaho
Bing	bing.com	https://www.bing.com/search?q=...
Ask	ask.com	https://www.ask.cor
AOL	aol.com	https://search.aol.c

Other search engines

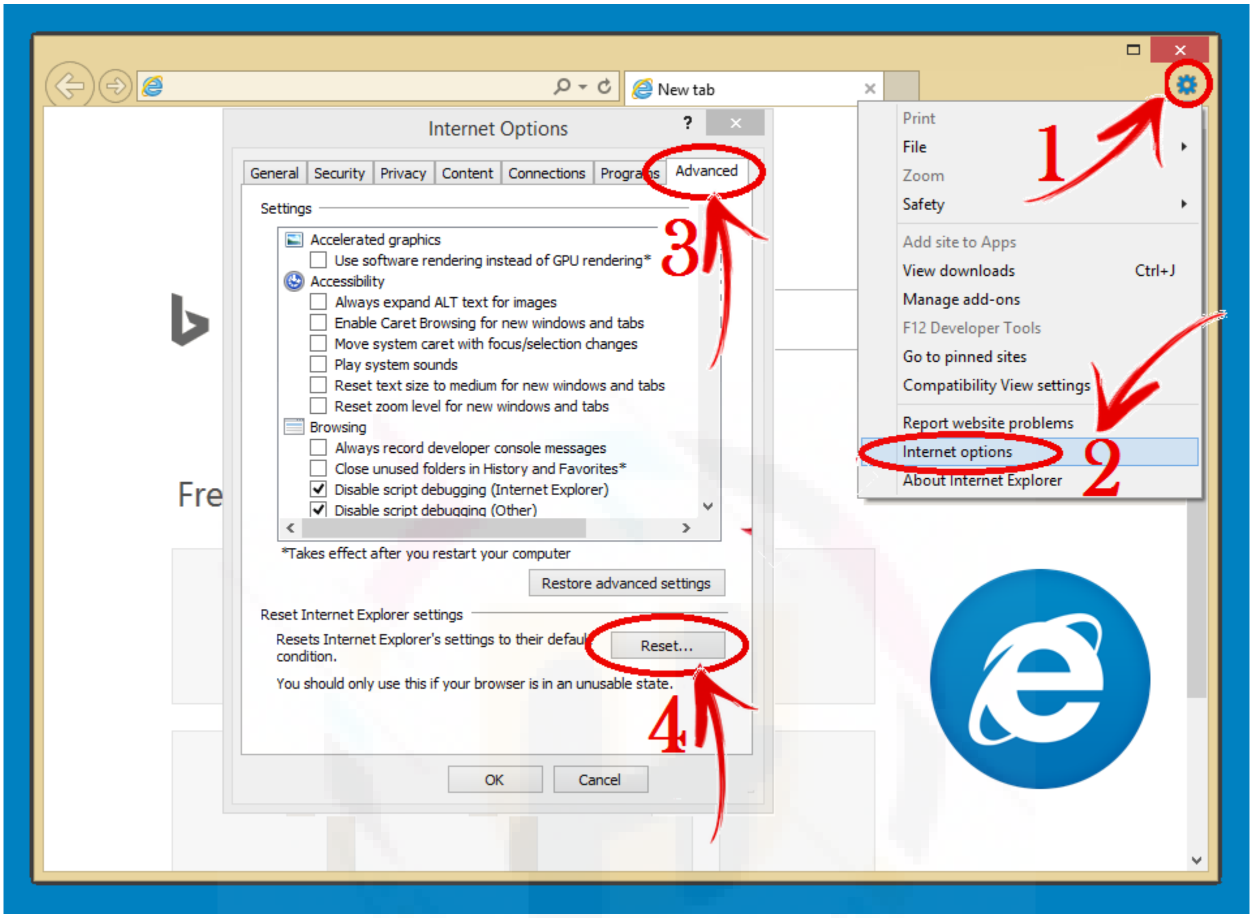
Search engine	Keyword	Query URL
Facebook	facebook.com	https://www.facebo
freepik.com	freepik.com	https://www.freepik.
Google Drive	drive.google.com	https://drive.google.com/drive/sea...
MvnRepository	mvnrepository.com	http://mvnrepository.com/search?...
Snapdeal.com	snapdeal.com	https://www.snapdeal.com/search...
YouTube Video Search	youtube.com	https://www.youtube.com/results?...

Reset Chrome Browser Search Engine 8

Reset Internet Explorer

1. Close all the opened tabs on the browser and then click on the “Tools” button → select “Internet options”.

2. Choose the “Advanced” tab, and then select “Reset”.
3. Reset Internet Explorer Settings dialog box will appear, select “Reset” to confirm.
4. Once finished, select “Close” → select “OK”. Restart your browser to apply changes.



Internet Options

Settings

Accelerated graphics
☐ Use software rendering instead of GPU rendering*
Accessibility
☐ Always expand ALT text for images
☐ Enable Caret Browsing for new windows and tabs
☐ Move system caret with focus/selection changes
☐ Play system sounds
☐ Reset text size to medium for new windows and tabs
☐ Reset zoom level for new windows and tabs
Browsing
☐ Always record developer console messages
☐ Close unused folders in History and Favorites*
☑ Disable script debugging (Internet Explorer)
☑ Disable script debugging (Other)

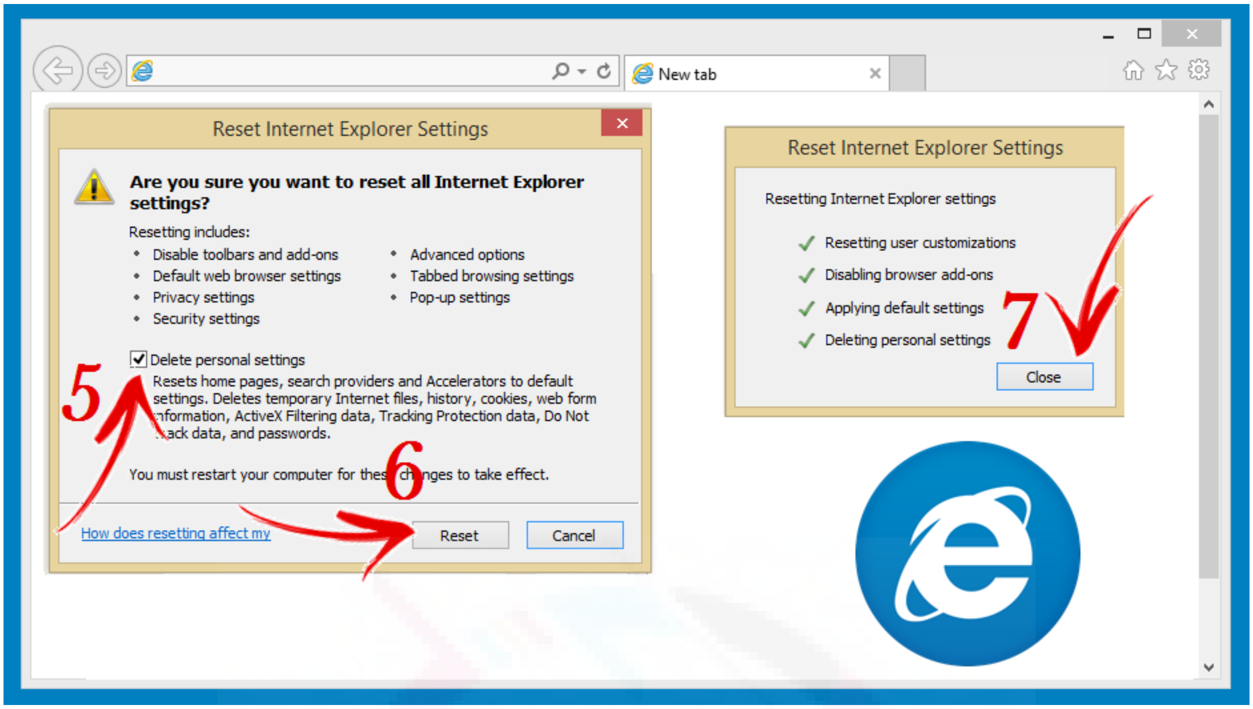
*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their defaul[t] condition.

You should only use this if your browser is in an unusable state.

Resetting Internet Explorer Image 1



Reset Internet Explorer Settings

Are you sure you want to reset all Internet Explorer settings?

Resetting includes:

- Disable toolbars and add-ons
- Default web browser settings
- Privacy settings
- Security settings
- Advanced options
- Tabbed browsing settings
- Pop-up settings

☑ Delete personal settings

Resets home pages, search providers and Accelerators to default settings. Deletes temporary Internet files, history, cookies, web form information, ActiveX Filtering data, Tracking Protection data, Do Not Track data, and passwords.

You must restart your computer for these changes to take effect.

How does resetting affect my

Reset Internet Explorer Settings

Resetting Internet Explorer settings

✓ Resetting user customizations

✓ Disabling browser add-ons

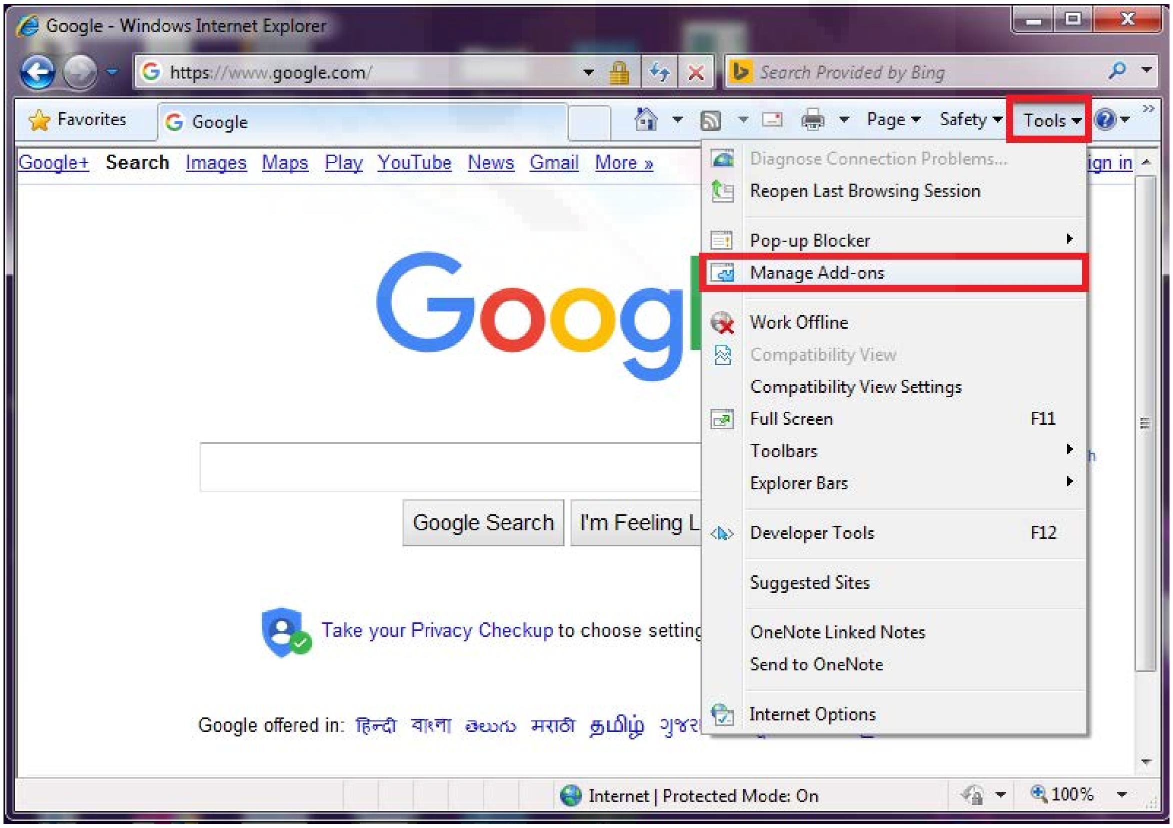
✓ Applying default settings

✓ Deleting personal settings

Resetting Internet Explorer Image 2

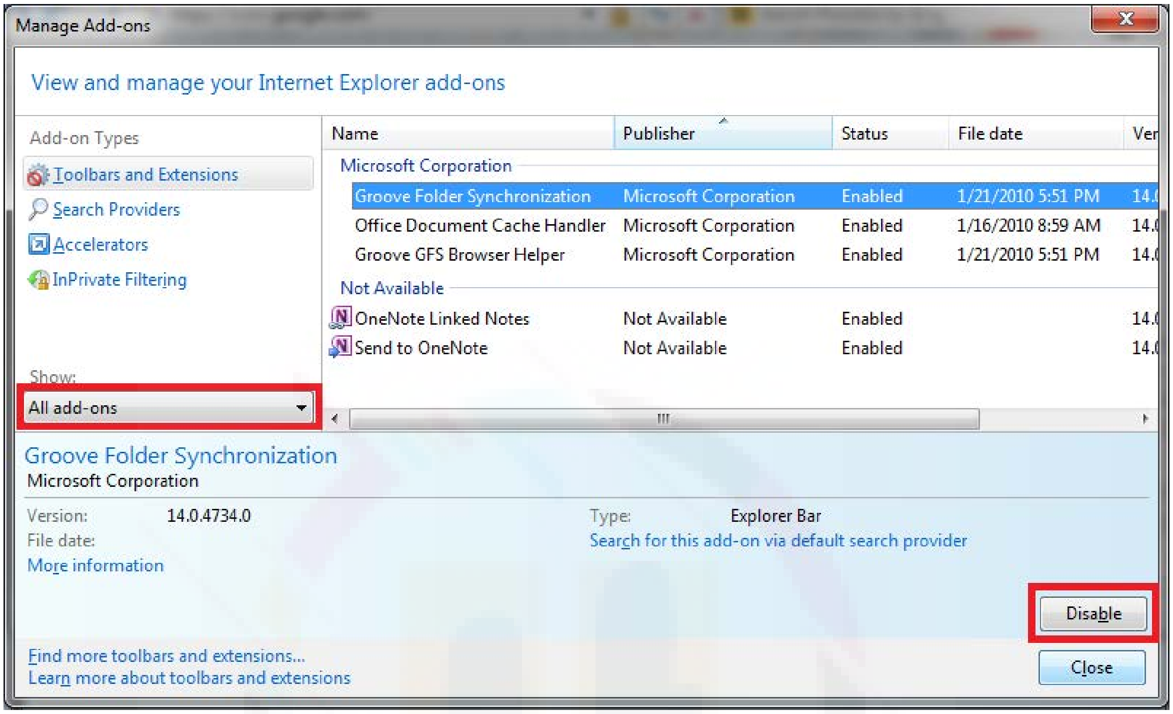
Removing unwanted extensions

1. On Internet Explorer browser click “Tools,” icon;



Remove add-ons From IE 1

2. Select “Manage add-ons.” Within the Manage add-ons window on show section choose “All add-ons”. This will list all the toolbars and extensions installed on the browser.
3. Select the ones which are unusual and can be recognized as an Adware;
4. Click “Disable.”



View and manage your Internet Explorer add-ons

Name	Publisher	Status	File date	Ver
Microsoft Corporation				
Groove Folder Synchronization	Microsoft Corporation	Enabled	1/21/2010 5:51 PM	14.
Office Document Cache Handler	Microsoft Corporation	Enabled	1/16/2010 8:59 AM	14.
Groove GFS Browser Helper	Microsoft Corporation	Enabled	1/21/2010 5:51 PM	14.
Not Available				
OneNote Linked Notes	Not Available	Enabled		14.
Send to OneNote	Not Available	Enabled		14.

Show: All add-ons

Groove Folder Synchronization
Microsoft Corporation

Version: 14.0.4734.0
File date:
More information

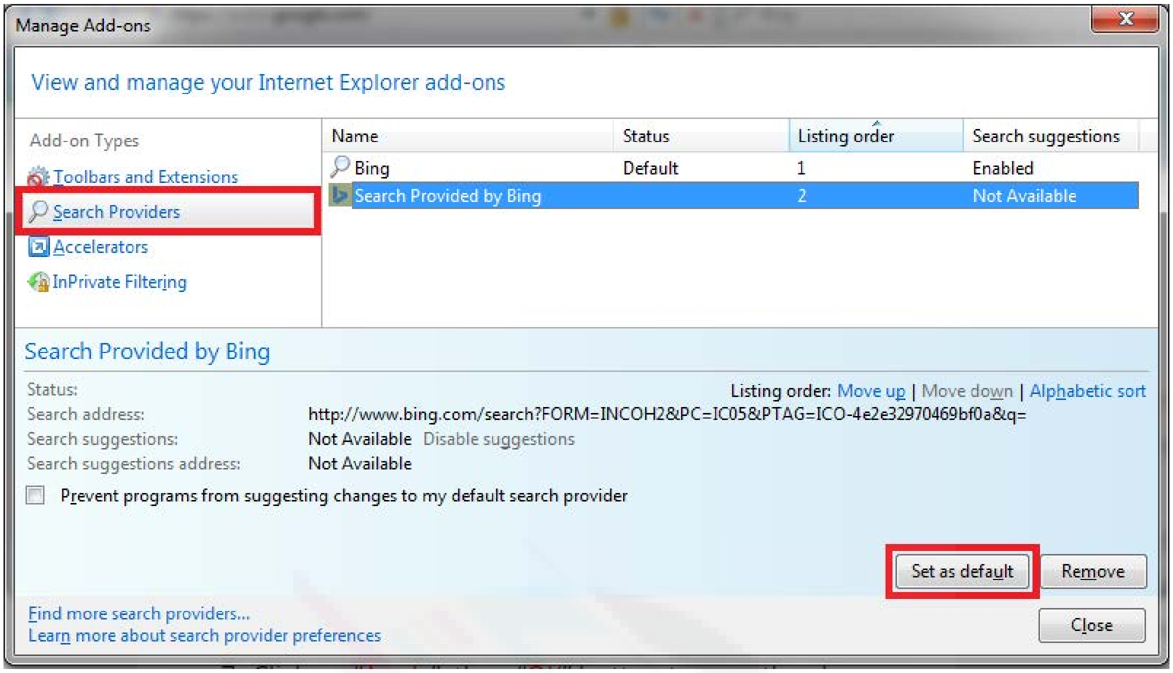
Type: Explorer Bar
Search for this add-on via default search provider

Remove add-ons From IE 2

5. Repeat the steps for all unwanted add-ons and extensions.

Check for existing start page, search engines, and other defaul ts.

1. On the same very window, click on “Search Providers”;
2. You will see the list of search engines, choose the ones which you like to “set as default”;



View and manage your Internet Explorer add-ons

Name	Status	Listing order	Search suggestions
Bing	Default	1	Enabled
Search Provided by Bing		2	Not Available

Search Provided by Bing

Status: Listing order: Move up | Move down | Alphabetic sort

Search address: http://www.bing.com/search?FORM=INCOH2&PC=IC05&PTAG=ICO-4e2e32970469bf0a&q=

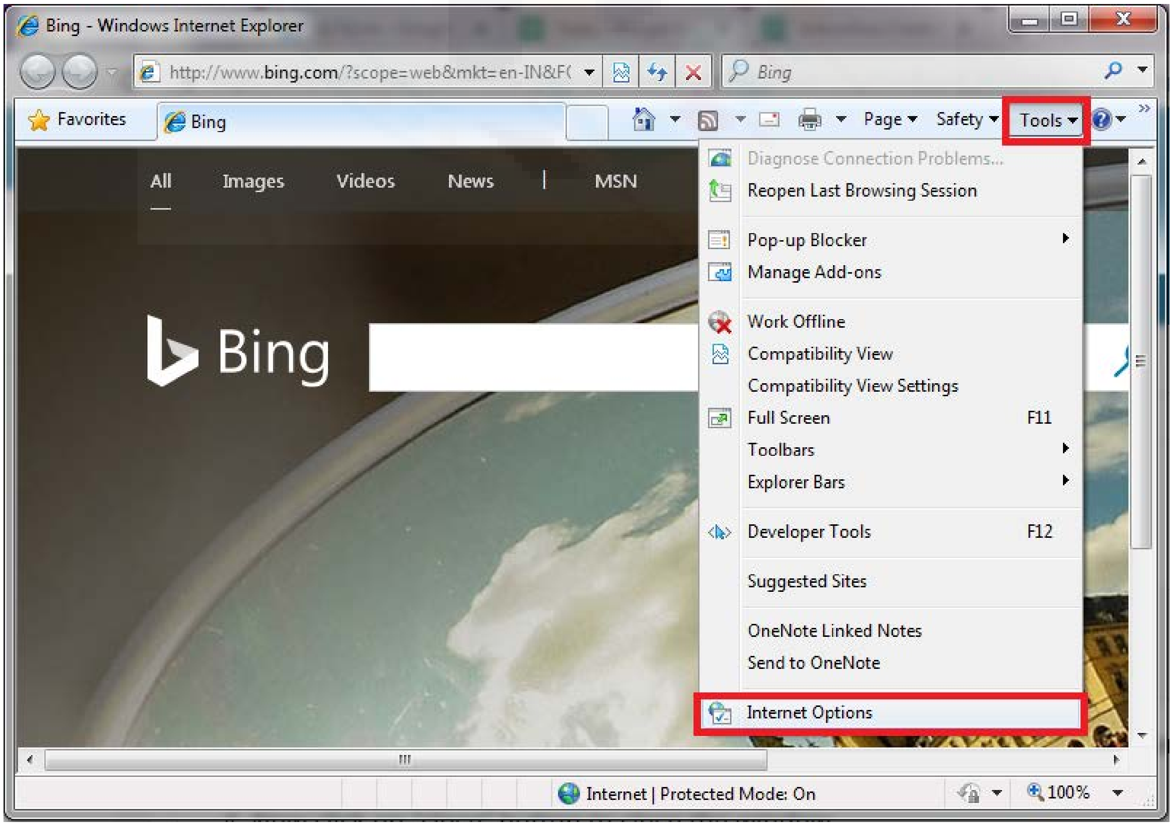
Search suggestions: Not Available Disable suggestions

Search suggestions address: Not Available

☐ Prevent programs from suggesting changes to my default search provider

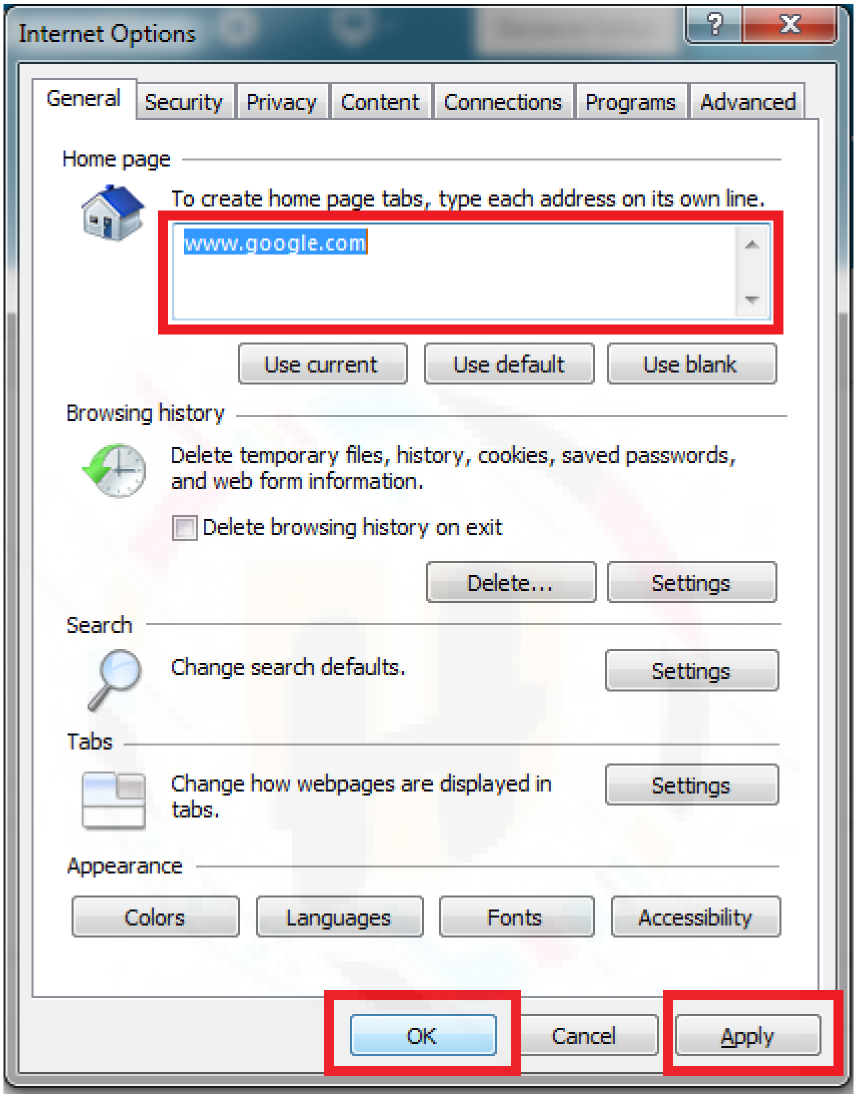
Resetting Search Engine From IE 3

3. Remove the Search engine which appears to be unknown by clicking on it and then click on “Remove”.
4. Now click on “close” button to close the window.
5. Next step is setting up your preferred homepage For this, Go to “Tools”, select “Internet Options”.



Resetting Search Engine From IE 5

6. Under the General tab, you will see ‘Homepage’ section, wherein you may see any unknown URL set as the default homepage, you need to replace it with your favorite ones like www.google.com or any other URL of your preference.
7. Click on “Apply”, then “OK” button to save the changes;



To create home page tabs, type each address on its own line.

www.google.com

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Change search defaults.

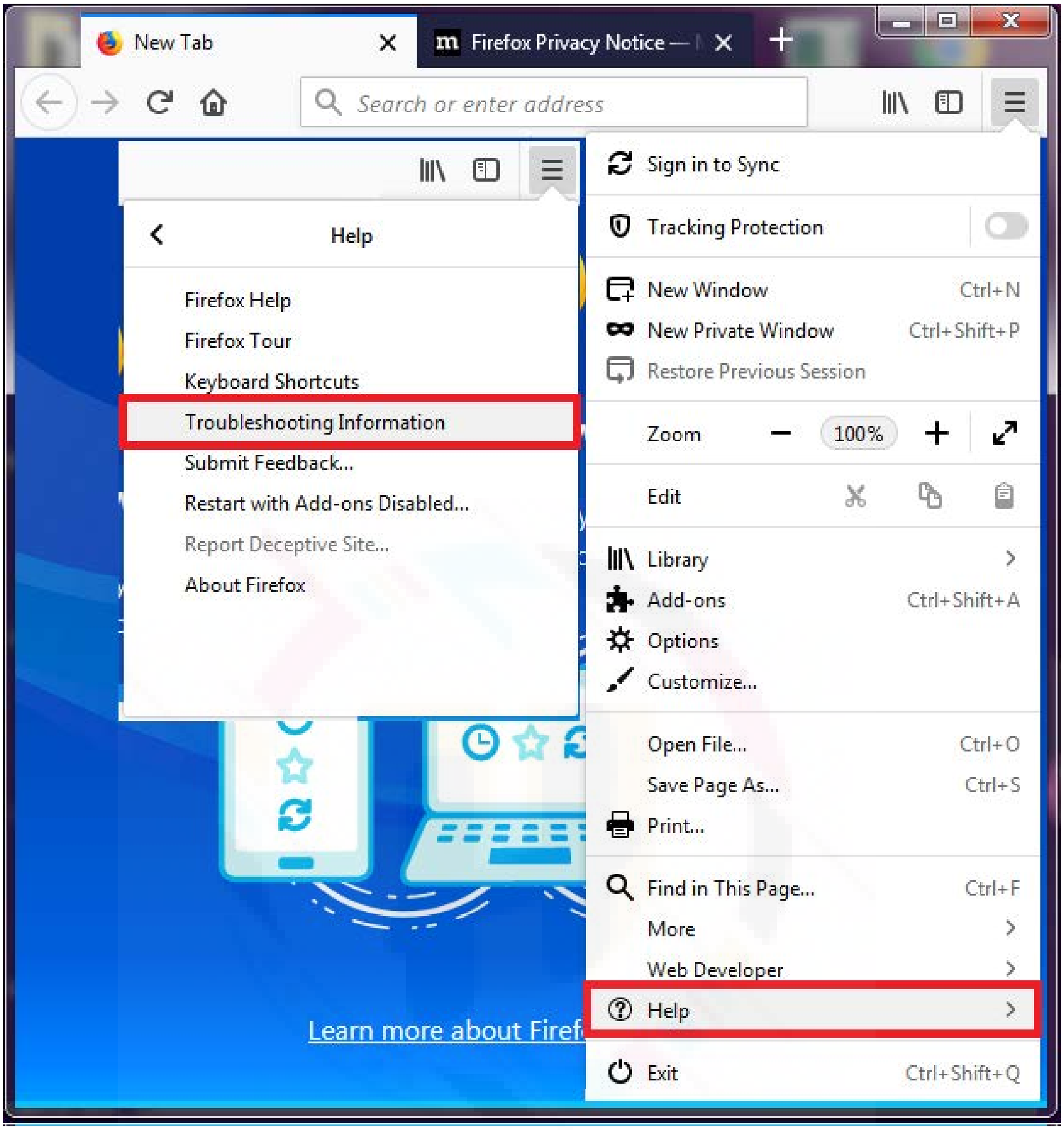
Change how webpages are displayed in tabs.

Add Default Page IE

8. Close this window and check if everything is working fine now.

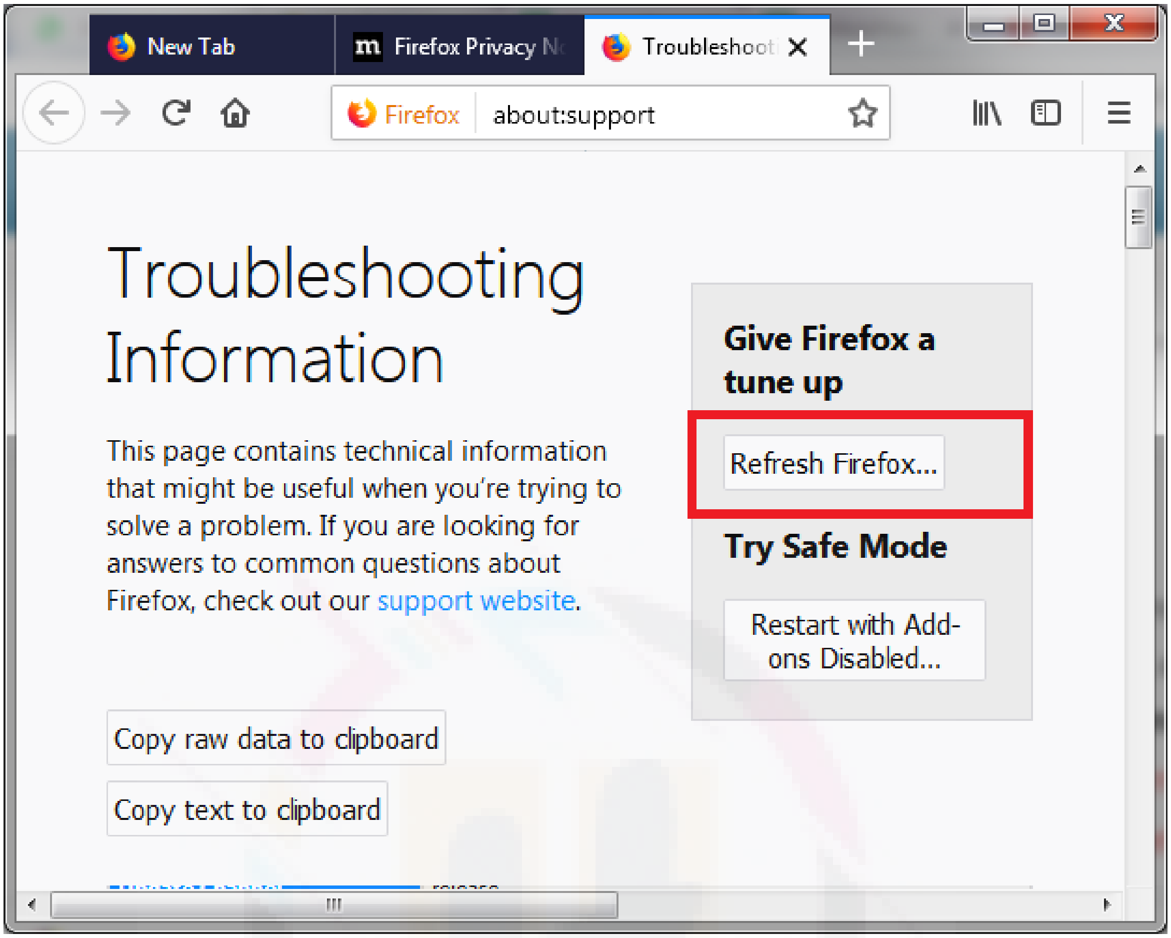
Reset Mozilla Firefox

1. Next step is resetting to the default settings on the Firefox, click the Firefox button→ go to the Help sub-menu→ select Troubleshooting Information (for Windows XP, click on the Help menu appearing at the top of the Firefox window). URL for troubleshooting Firefox is “about:support”(copy and paste this URL to the Firefox browser).



Reset Mozilla Firefox Step 1

2. On the upper-right corner of the Troubleshooting Informationpage click on the “Reset Firefox” button.

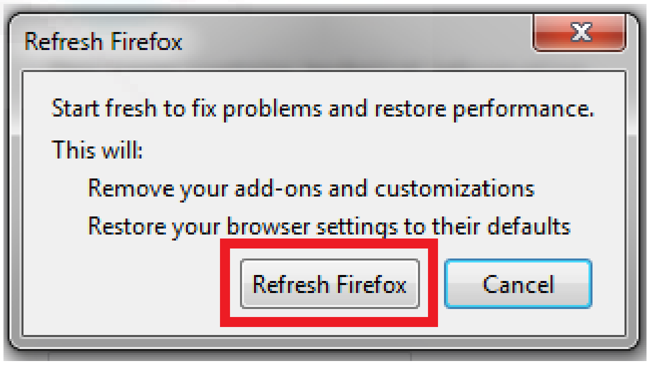


Troubleshooting Information

This page contains technical information that might be useful when you're trying to solve a problem. If you are looking for answers to common questions about Firefox, check out our support website.

Reset Mozilla Firefox Step 2

3. When the confirmation window appears click on "Reset Firefox". This will close the Firefox browser and will reset to the default settings.
4. After reset, a window will appear listing all the information about the imported. Now click on Finish.



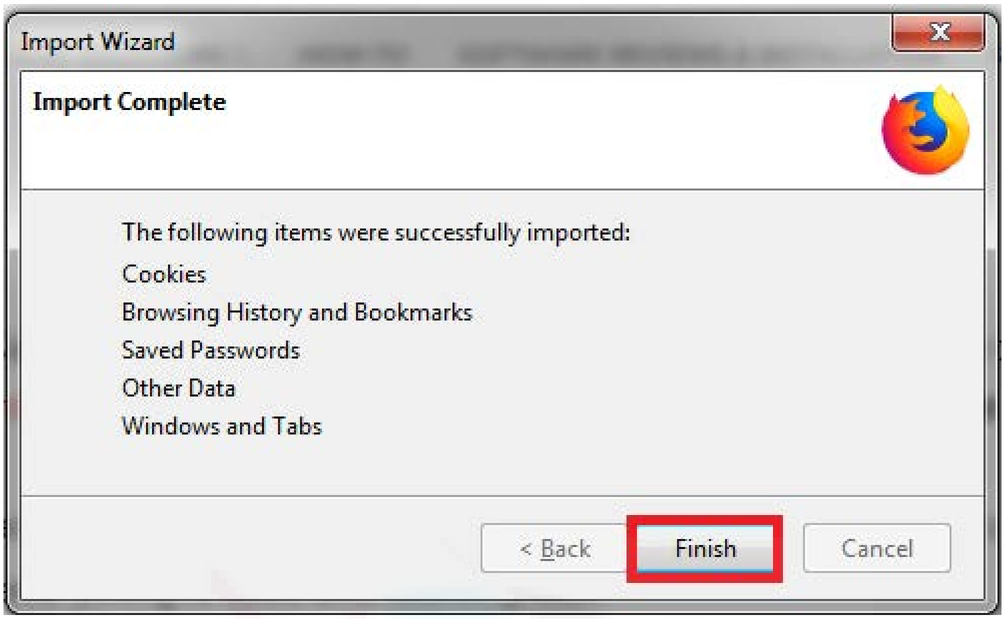
Start fresh to fix problems and restore performance.

This will:

Remove your add-ons and customizations

Restore your browser settings to their defaults

Reset Mozilla Firefox Step 3



Import Complete

The following items were successfully imported:

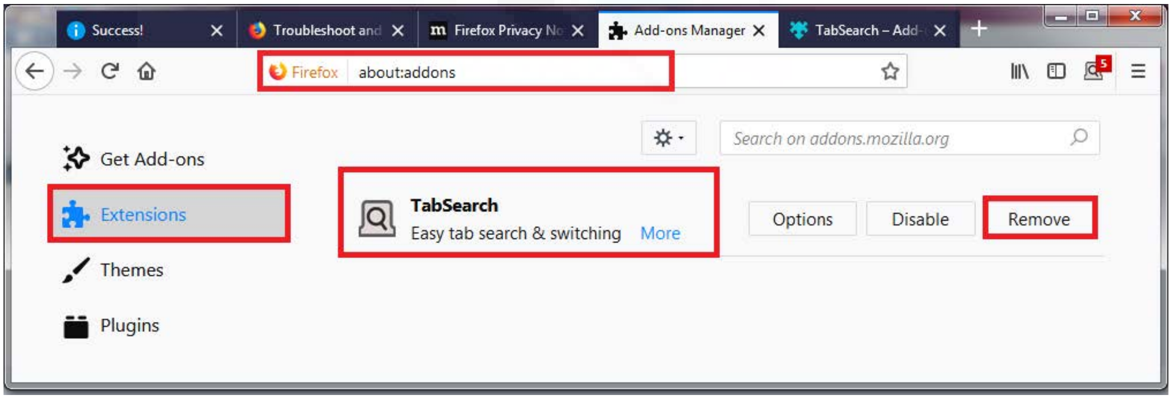
Cookies
Browsing History and Bookmarks
Saved Passwords
Other Data
Windows and Tabs

Reset Mozilla Firefox Step 4

5. Restart the browser to check if everything is fixed and working well.

Removing unwanted extensions

1. Start your Firefox browser and click on three horizontal lines on the top right corner to open menu then select “Add-ons”. You can also press Ctrl+Shift+A on your keyboard or copy and paste “about:addons” to the address bar to open the ‘Add-Ons Manager’ page. This page will show you the list of all extensions/add-ons installed on your browser.
2. Select Extensions, and check the installed extensions and if it stands out to be an Adware/PUP then click on Remove button.



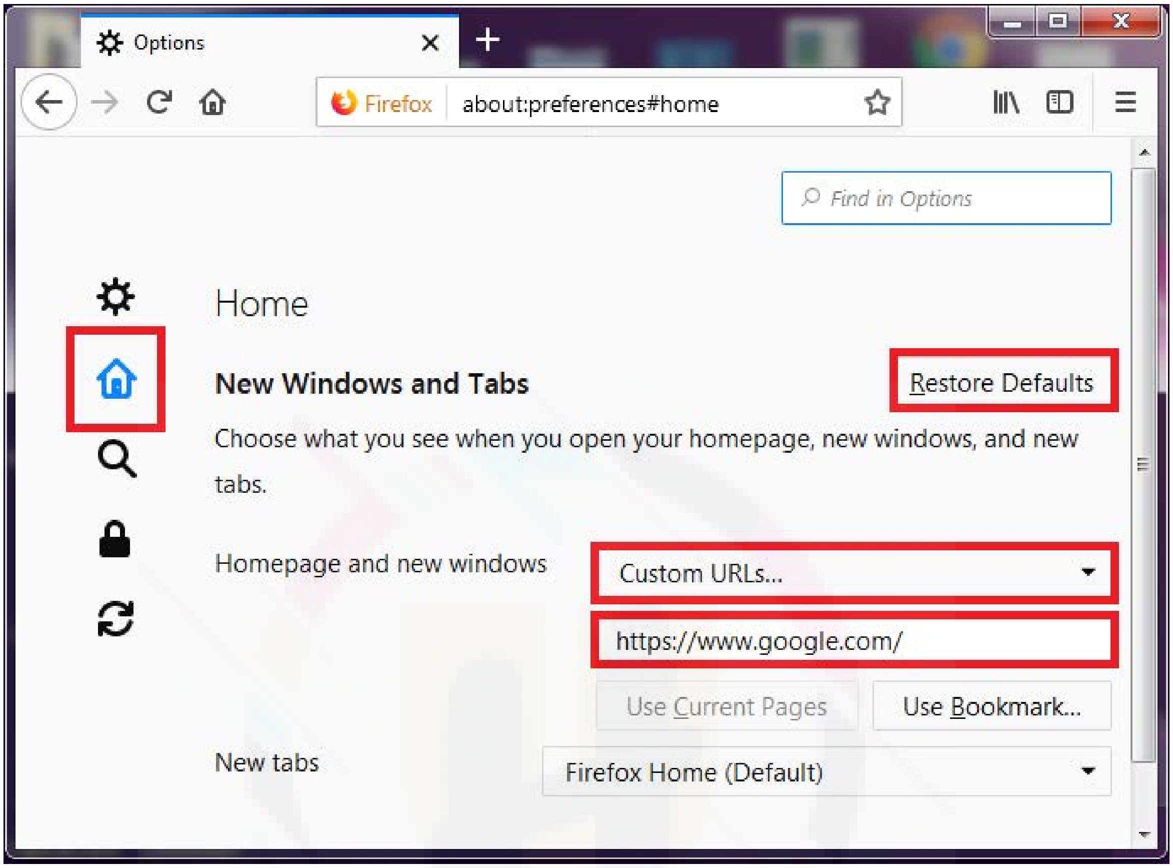
Remove Addons From Firefox 1

3. You may be prompted to restart the browser then do it make the changes successful.

Check for existing start page, search engines, and other defaul ts

1. Again go to Menu by clicking on three horizontal lines at the top-right corner of the browser;

2. Select "Options" then switch to the General Tab and reset the default homepage or simply go to URL "about:preferences#home".
3. You can simply "Restore Defaults" or set your custom homepage. follow the below image.

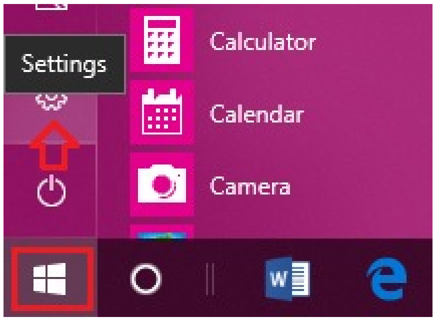


Reset Mozilla Firefox Default Pages

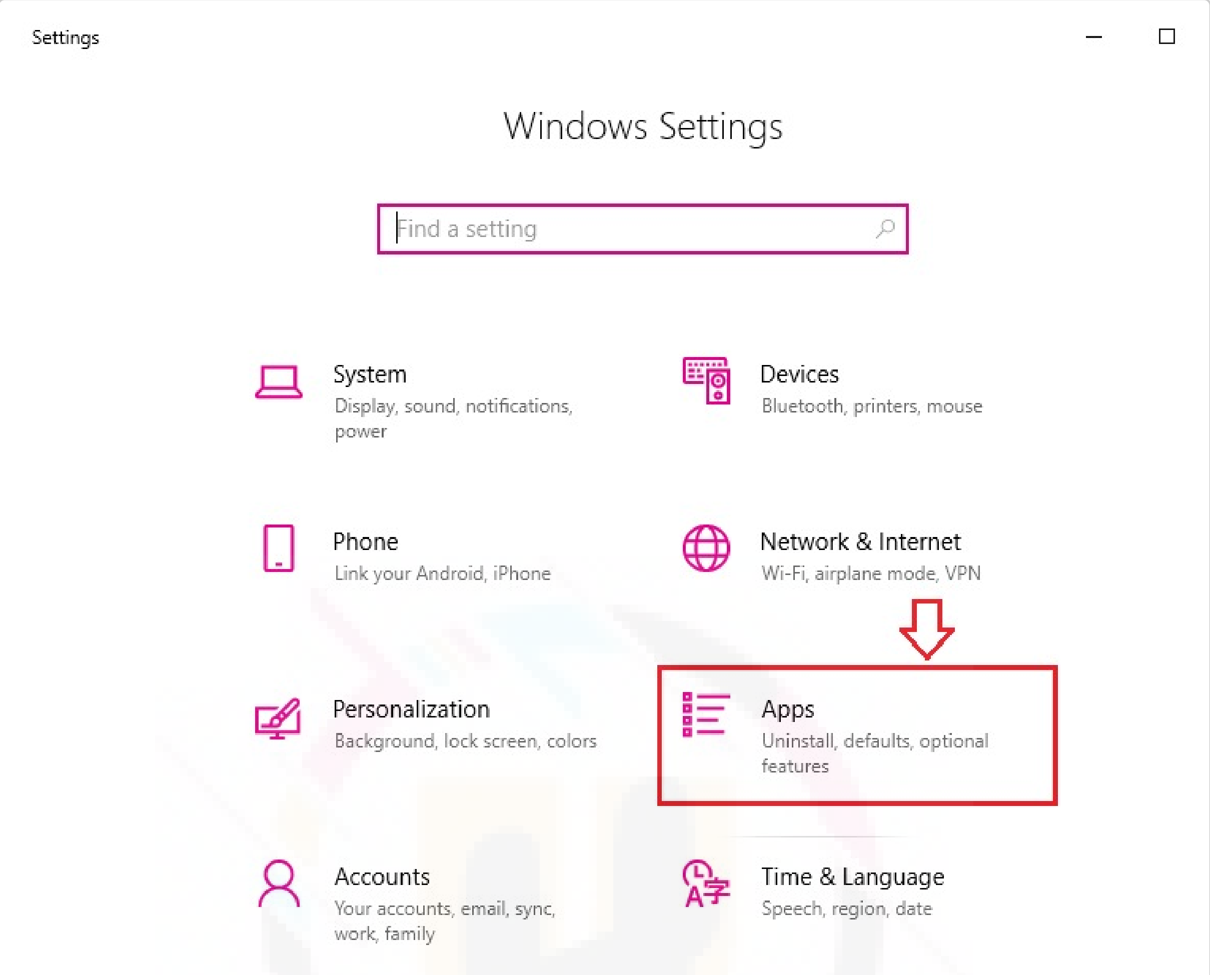
Reset Microsoft Edge

Microsoft Edge is a built-in browser for windows 10 which has lots of features like accessing windows app within the browser too. It uses bing search as default to carry out searches within. And the extensions here can be installed from the Microsoft App store. But still if get any Adware installed within Microsoft Edge browser then follow the steps to reset the browser.

1. Right-click on the "Start" and select "Settings";
2. Go to "Apps and Features";

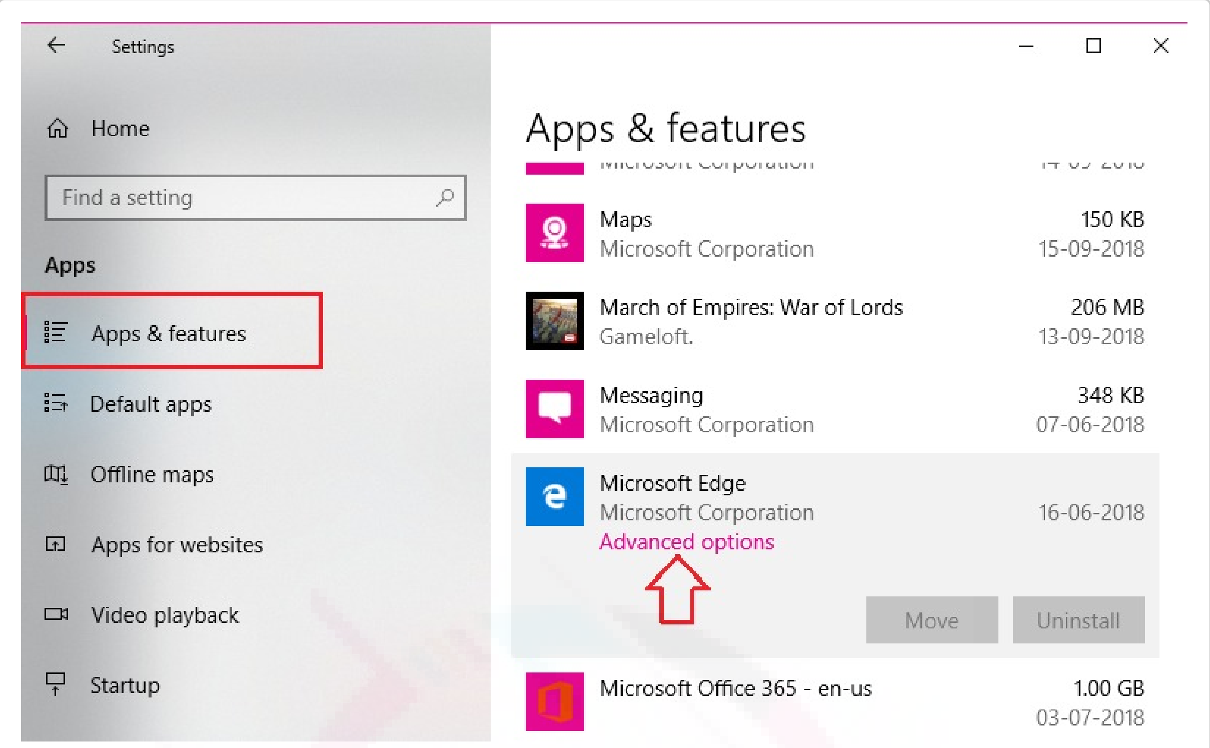


Reset Microsoft Edge Step 1


Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date

Reset Microsoft Edge Step 2

3. Choose "Microsoft Edge" from the list of programs;
4. Clicking on will expand the program now click on "Advanced Option"



Settings

Home

Find a setting

Apps

Apps & features

Default apps

Offline maps

Apps for websites

Video playback

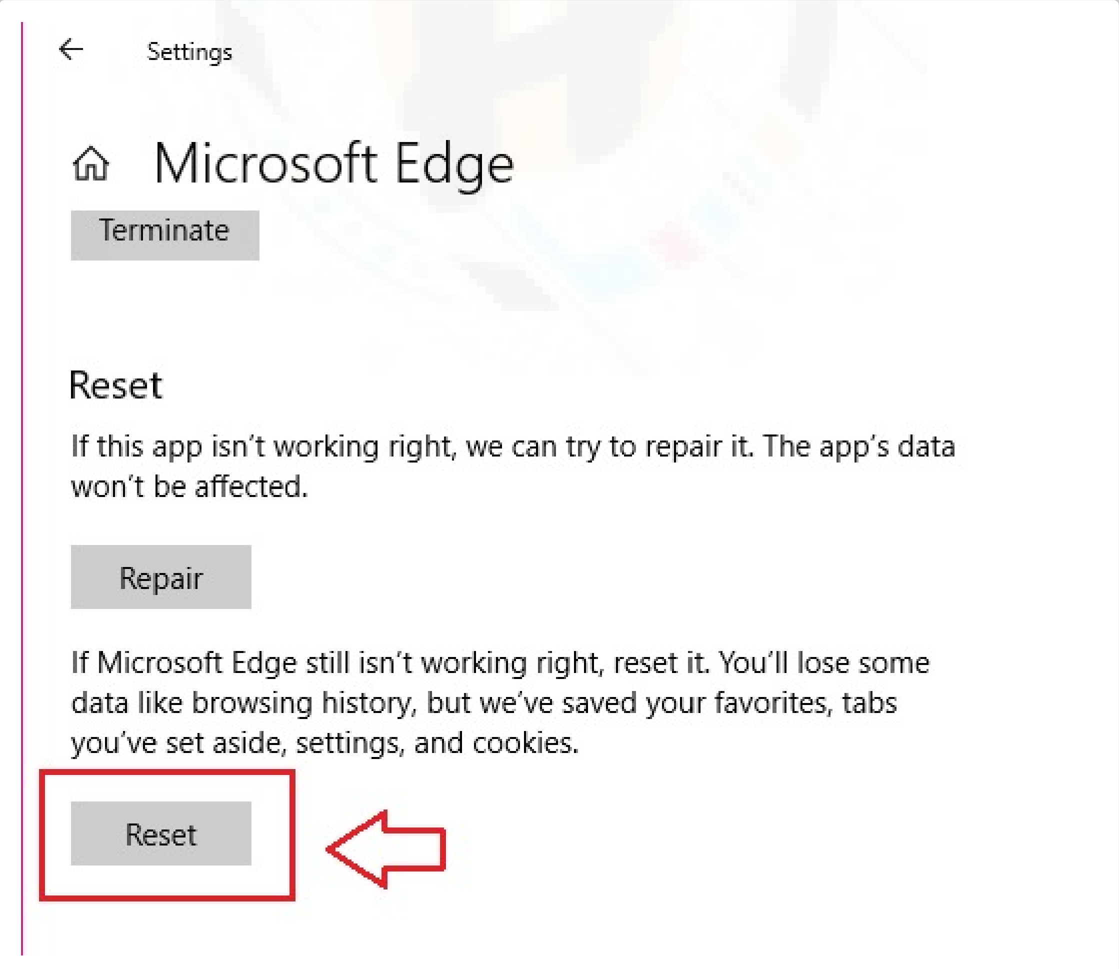
Startup

Apps & features

Maps Microsoft Corporation	150 KB 15-09-2018
March of Empires: War of Lords Gameloft.	206 MB 13-09-2018
Messaging Microsoft Corporation	348 KB 07-06-2018
Microsoft Edge Microsoft Corporation Advanced options	16-06-2018
Microsoft Office 365 - en-us	1.00 GB 03-07-2018

Reset Microsoft Edge Step 3

5. Scroll down to find Reset section, now click on “Reset” button.



Settings

Microsoft Edge

Reset

If this app isn’t working right, we can try to repair it. The app’s data won’t be affected.

If Microsoft Edge still isn’t working right, reset it. You’ll lose some data like browsing history, but we’ve saved your favorites, tabs you’ve set aside, settings, and cookies.

Reset Microsoft Edge Step 4

Step 3 & 4: Remove Trojan virus using System Restore Procedure

1. Reboot your computer to "Safe Mode with Command Prompt"
2. Windows 7 / Vista / XP
   - Click Start → Restart → OK.
   - When your computer becomes active, start pressing "F8" multiple times until you see the Advanced Boot Optionswindow.
   - Select Command Promptfrom the list

   Windows 10 / Windows 8

   - Press the Power buttonat the Windows login screen. Now press and hold Shift, which is on your keyboard, and click Restart.
   - Now select Troubleshoot→ Advanced options</em class="uhimpo"> → Startup Setting and finally press Restart.
   - Once your computer becomes active, select Enable Safe Mode with Command Promptin Startup Settings window.
3. Restore your system to default settings as it was prior to the Trojan attack
4. Once the Command Prompt window appears, type "cd restore" and press Enter.
5. Now again type "rstrui.exe" and hit Enter button;
6. It will show up a new window, now click on "Next" and select your restore point that should be prior to the attack of Trojan threat. Click on "Next".
7. Now click on "Yes" to confirm the system restore.
8. Once the system restores to your selected date is done, then you need to restart your computer normally.
9. Download effective anti-virus program and scan your computer to ensure successful removal of Trojan threat.

Use SpyHunter To Remove Trojan Virus

SpyHunter is a giant among the security programs that use advanced threat detection technology to remove any sort of Adware/PUPs, Browser hijacker, Trojans, Rootkits, Fake system optimization tools, worms, and rootkits.

It not only removes the threat but provides rigorous 24/7 protection from any unsolicited programs, vulnerability or rootkits attacks.

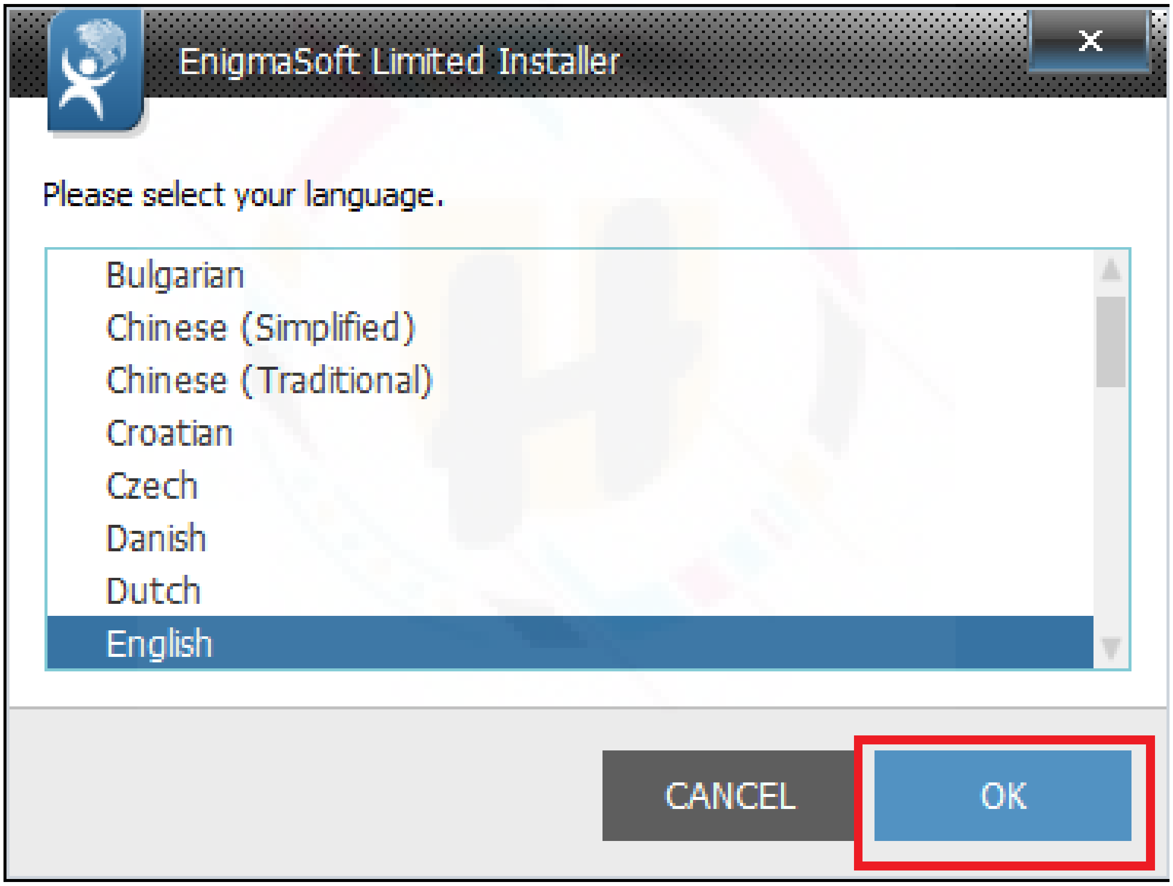
Why we are recommending SpyHunter is because of its efficiency, lightweight that only takes up 12% of the CPU space and simpler user-interface that is designed for both beginners and advanced users. Besides that, it has features which require less-user monitoring, custom scan options, system guard and 24*7 help desk support. Keeping SpyHunter actively running on your computer adds an extra security layer that protects your computer system from being attacked.

Spyhunter certified by "West Coast Labs' Checkmark Certification System" gives you a complete money-back guarantee, if you are not satisfied with its results. Because they are sure you will going to have it on your system. So, it's a win-win situation for you try out SpyHunter free version and if you are fully satisfied get registered for full protection against all malicious odds that hampers your security.

Instructions To Download An d Install SpyHunter 5

- Once the file “SpyHunter-Installer.exe” is downloaded, double-click on the file to open (you can see it in your browser’s bottom-left corner);
- Click “Yes” to the “User Account Control” dialog box;
- Now, choose your preferred language and then click on “OK” for the next installation step;

Download SpyHunter



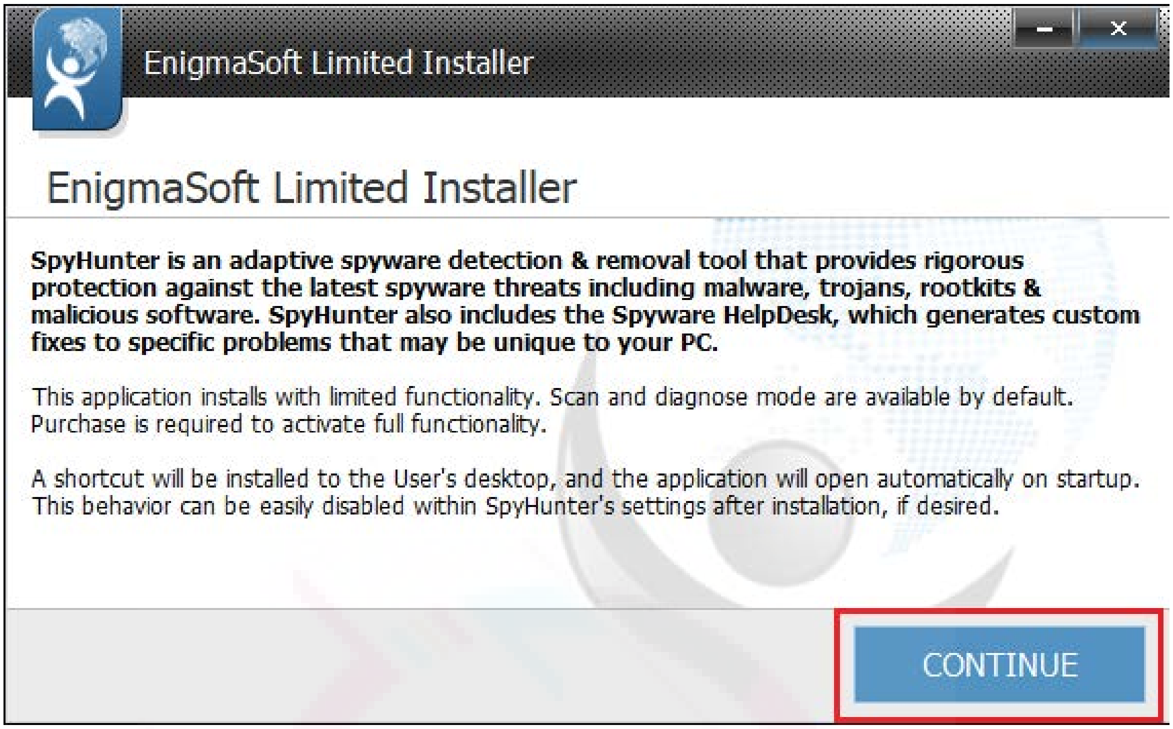
EnigmaSoft Limited Installer

Please select your language.

- Bulgarian
- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Czech
- Danish
- Dutch
- English

SpyHunter 5 Installation Step 1

- Now, click on the “Continue” button to proceed with the To proceed to the installation;



EnigmaSoft Limited Installer

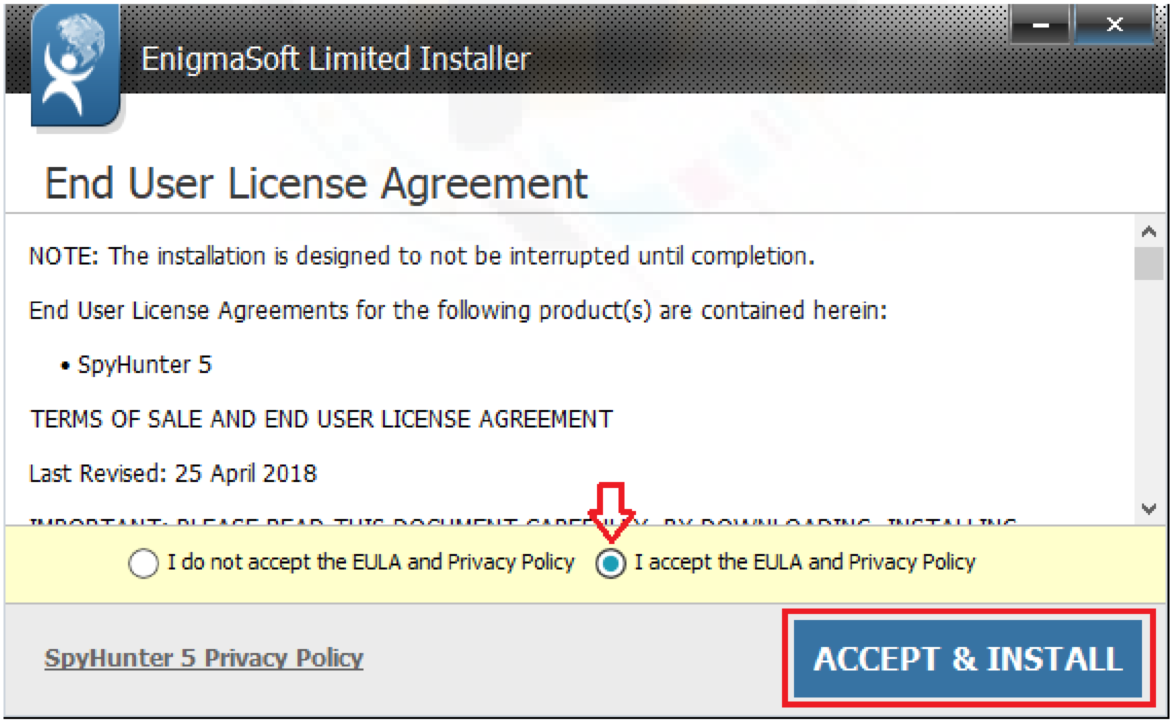
SpyHunter is an adaptive spyware detection & removal tool that provides rigorous protection against the latest spyware threats including malware, trojans, rootkits & malicious software. SpyHunter also includes the Spyware HelpDesk, which generates custom fixes to specific problems that may be unique to your PC.

This application installs with limited functionality. Scan and diagnose mode are available by default. Purchase is required to activate full functionality.

A shortcut will be installed to the User's desktop, and the application will open automatically on startup. This behavior can be easily disabled within SpyHunter's settings after installation, if desired.

SpyHunter 5 Installation Step 2

- Read and click on the accept button to agree for “End User License Agreement” and “Privacy Policy”. Now, click on the “Install” button.



End User License Agreement

NOTE: The installation is designed to not be interrupted until completion.

End User License Agreements for the following product(s) are contained herein:

- SpyHunter 5

TERMS OF SALE AND END USER LICENSE AGREEMENT

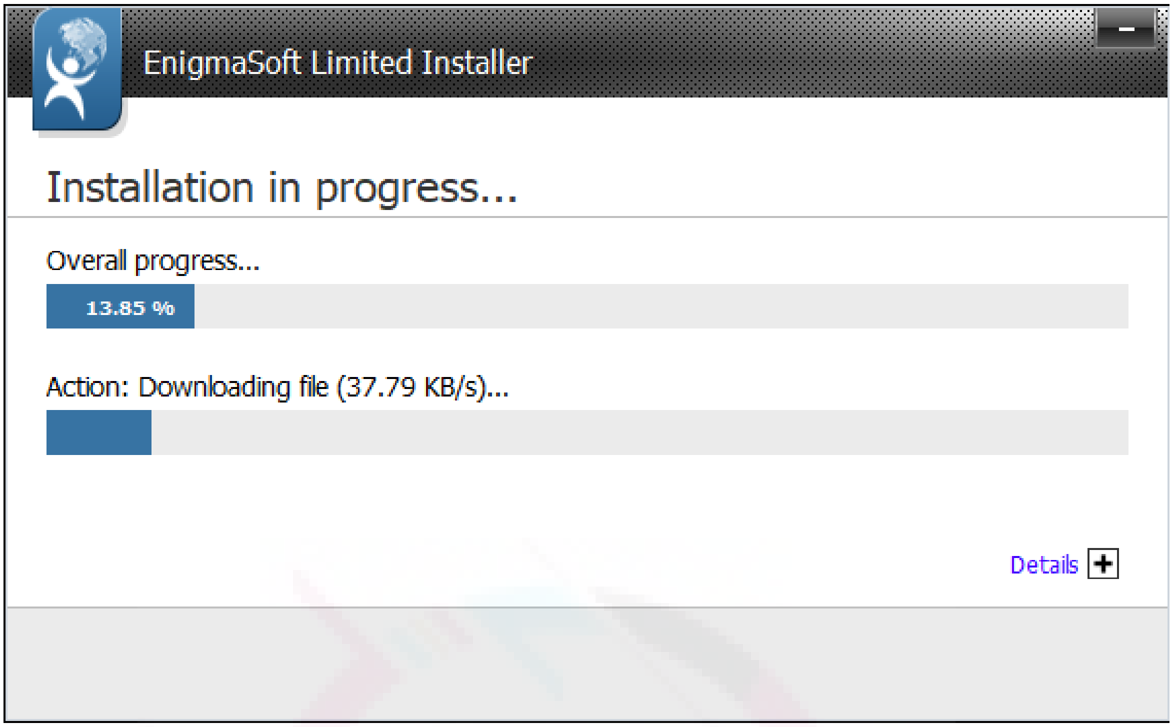
Last Revised: 25 April 2018

IMPORTANT: PLEASE READ THIS DOCUMENT CAREFULLY. BY DOWNLOADING, INSTALLING

○ I do not accept the EULA and Privacy Policy ● I accept the EULA and Privacy Policy

SpyHunter 5 Installation Step 4

- Now installation will begin, please be patience as it may take few minutes;



Installation in progress...

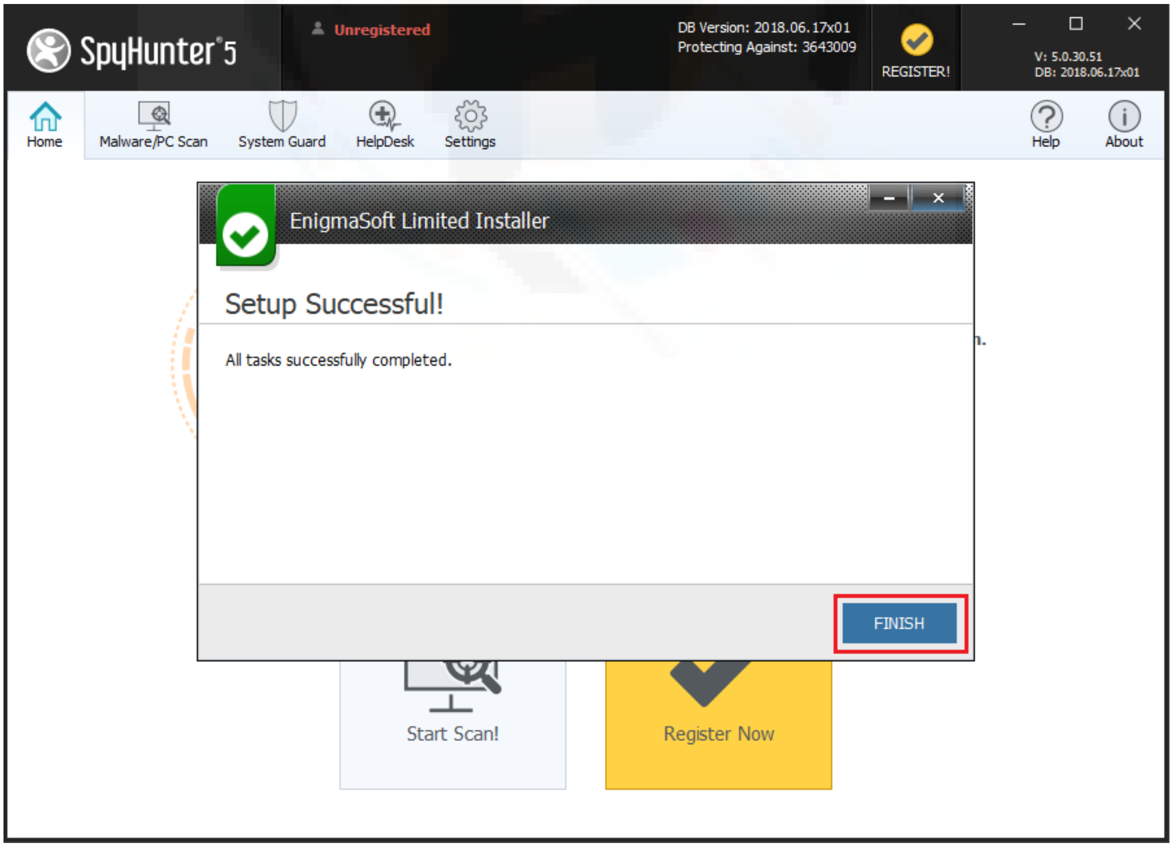
Overall progress...

13.85 %

Action: Downloading file (37.79 KB/s)...

SpyHunter 5 Installation Step 5

- Click on the “Finish” button to successfully install the program.



Setup Successful!

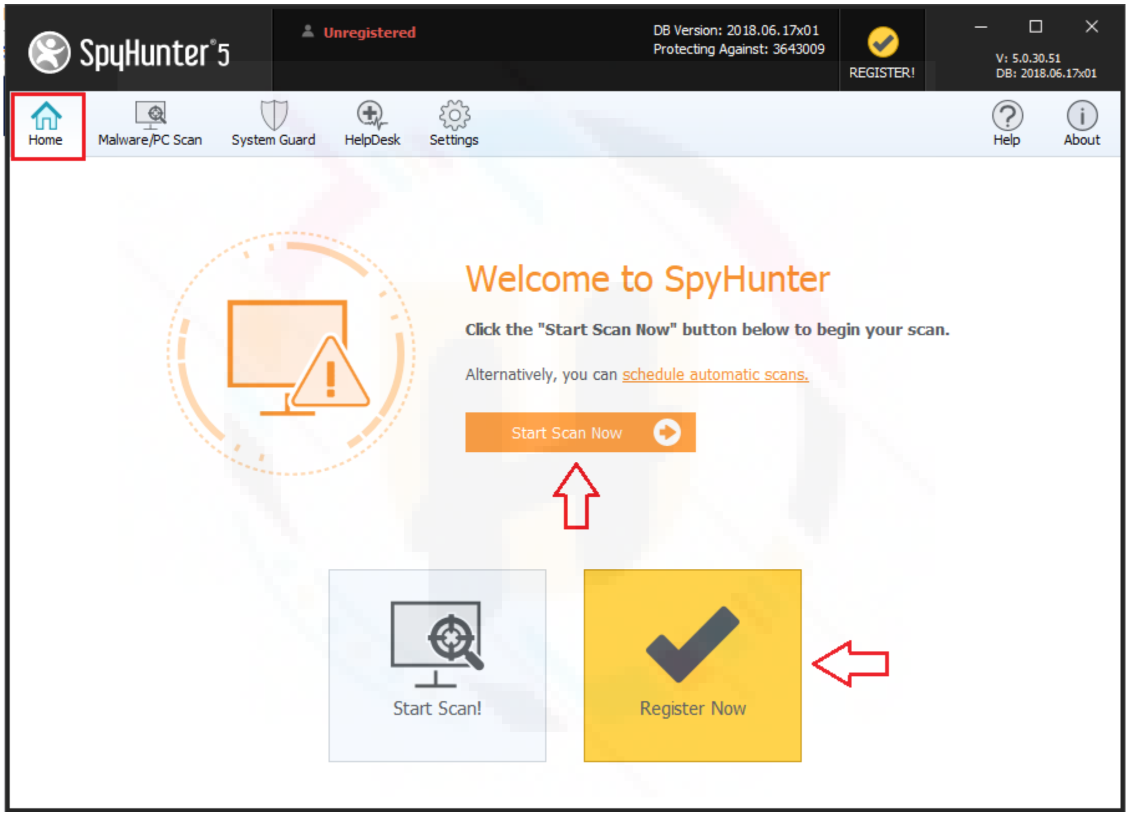
All tasks successfully completed.

SpyHunter 5 Installation Step 6

Note: It may ask you to enter your information- there you can add your details or go with the default information to start the program.

Steps To Perform System Scan with SpyHunter

- Once the program is installed successfully, the SpyHunter 5 Anti-malware program will launch automatically. If it does not then locate the SpyHunter icon on the desktop or click on “Start” → “Programs” → Select “SpyHunter”.
- Now, To start the scan click on the “Home” tab and select “Start Scan Now” button. The program will now start scanning for threats, malware, unwanted programs, rootkits, and system vulnerabilities.



Welcome to SpyHunter

Click the "Start Scan Now" button below to begin your scan.

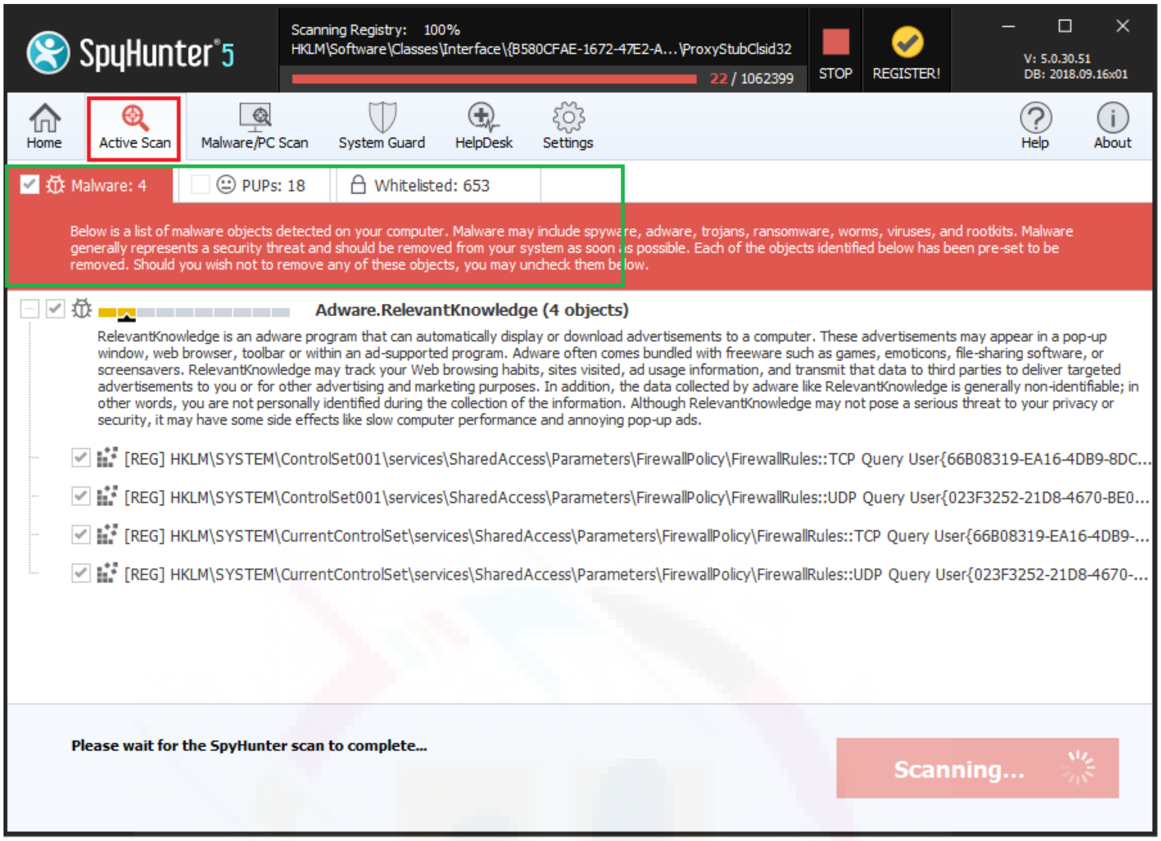
Alternatively, you can schedule automatic scans.

DB Version: 2018.06.17x01
Protecting Against: 3643009

V: 5.0.30.51
DB: 2018.06.17x01

SpyHunter 5 Start Scan Now

- The scan will report will all the details of the result along with system errors, vulnerabilities and malware found.



Scanning Registry: 100%
HKLM\Software\Classes\Interface\{B580CFAE-1672-47E2-A...\ProxyStubClsid32
22 / 1062399

V: 5.0.30.51
DB: 2018.09.16x01

Below is a list of malware objects detected on your computer. Malware may include spyware, adware, trojans, ransomware, worms, viruses, and rootkits. Malware generally represents a security threat and should be removed from your system as soon as possible. Each of the objects identified below has been pre-set to be removed. Should you wish not to remove any of these objects, you may uncheck them below.

☑ **Adware.RelevantKnowledge (4 objects)**

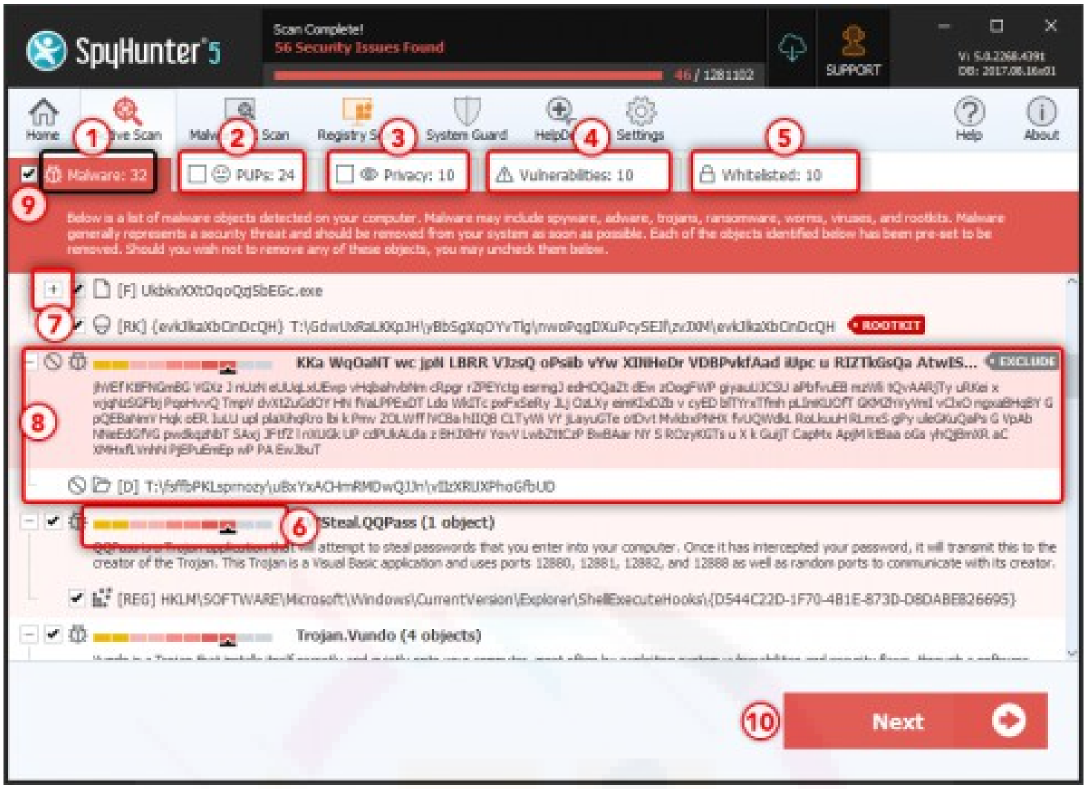
RelevantKnowledge is an adware program that can automatically display or download advertisements to a computer. These advertisements may appear in a pop-up window, web browser, toolbar or within an ad-supported program. Adware often comes bundled with freeware such as games, emoticons, file-sharing software, or screensavers. RelevantKnowledge may track your Web browsing habits, sites visited, ad usage information, and transmit that data to third parties to deliver targeted advertisements to you or for other advertising and marketing purposes. In addition, the data collected by adware like RelevantKnowledge is generally non-identifiable; in other words, you are not personally identified during the collection of the information. Although RelevantKnowledge may not pose a serious threat to your privacy or security, it may have some side effects like slow computer performance and annoying pop-up ads.

```
☑ [REG] HKLM\SYSTEM\ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules::TCP Query User{66B08319-EA16-4DB9-8DC...
☑ [REG] HKLM\SYSTEM\ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules::UDP Query User{023F3252-21D8-4670-BE0...
☑ [REG] HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules::TCP Query User{66B08319-EA16-4DB9-...
☑ [REG] HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules::UDP Query User{023F3252-21D8-4670-...
```

Please wait for the SpyHunter scan to complete...

SpyHunter 5 Malware Result

- SpyHunter 5 groups your scan results into categories determined by the type of objects detected: “Malware ”, “PUPs ” (Potentially Unwanted Programs), “Privacy ”, “Vulnerabilities ”, and “Whitelisted objects ”, as shown in the screenshot below:


SpyHunter 5
Scan Complete!
56 Security Issues Found
46 / 1281102
SUPPORT
V: 5.0.2268.4391
DB: 2017.08.16.01
Home
Active Scan
Malware/PC Scan
Registry Scan
System Guard
HelpDesk
Settings
Help
About
1
2
3
4
5
6
7
8
9
10
Malware: 32
PUPs: 24
Privacy: 10
Vulnerabilities: 10
Whitelisted: 10
[F] UkbkvXXtOqoQzjSbEGc.exe
[RK] {evkJlkaXbCnDcQH} T:\GdwUxRaLKKpJH\yBbSgXqOYvTlg\nwoPqgDXuPcySEJf\zvJXM\evkJlkaXbCnDcQH
ROOTKIT
KKa WqOaNT wc jpN LBRR VJzsQ oPsib vYw XINHeDr VDBPvkfAad iUpc u RIZTkGsQa AtwIS...
EXCLUDE
[D] T:\fsffbPKLspmozy\uBxYxACHmRMDwQJJn\vIlzXRUXPhoGfbUD
Steal.QQPass (1 object)
[REG] HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks\{D544C22D-1F70-481E-873D-D8DABE826695}
Trojan.Vundo (4 objects)
Next

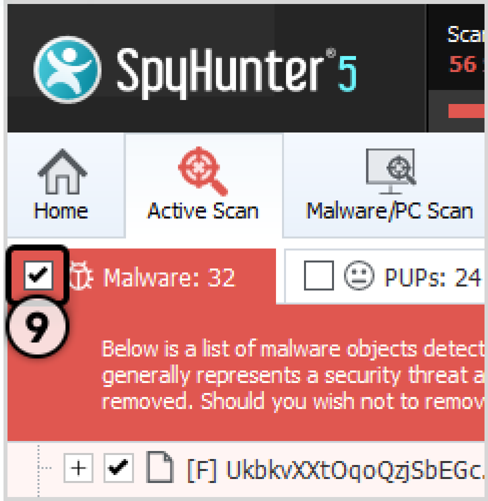
Below is a list of malware objects detected on your computer. Malware may include spyware, adware, trojans, ransomware, worms, viruses, and rootkits. Malware generally represents a security threat and should be removed from your system as soon as possible. Each of the objects identified below has been pre-set to be removed. Should you wish not to remove any of these objects, you may uncheck them below.

QQPass is a Trojan application that will attempt to steal passwords that you enter into your computer. Once it has intercepted your password, it will transmit this to the creator of the Trojan. This Trojan is a Visual Basic application and uses ports 12880, 12881, 12882, and 12888 as well as random ports to communicate with its creator.

SpyHunter Scan Result

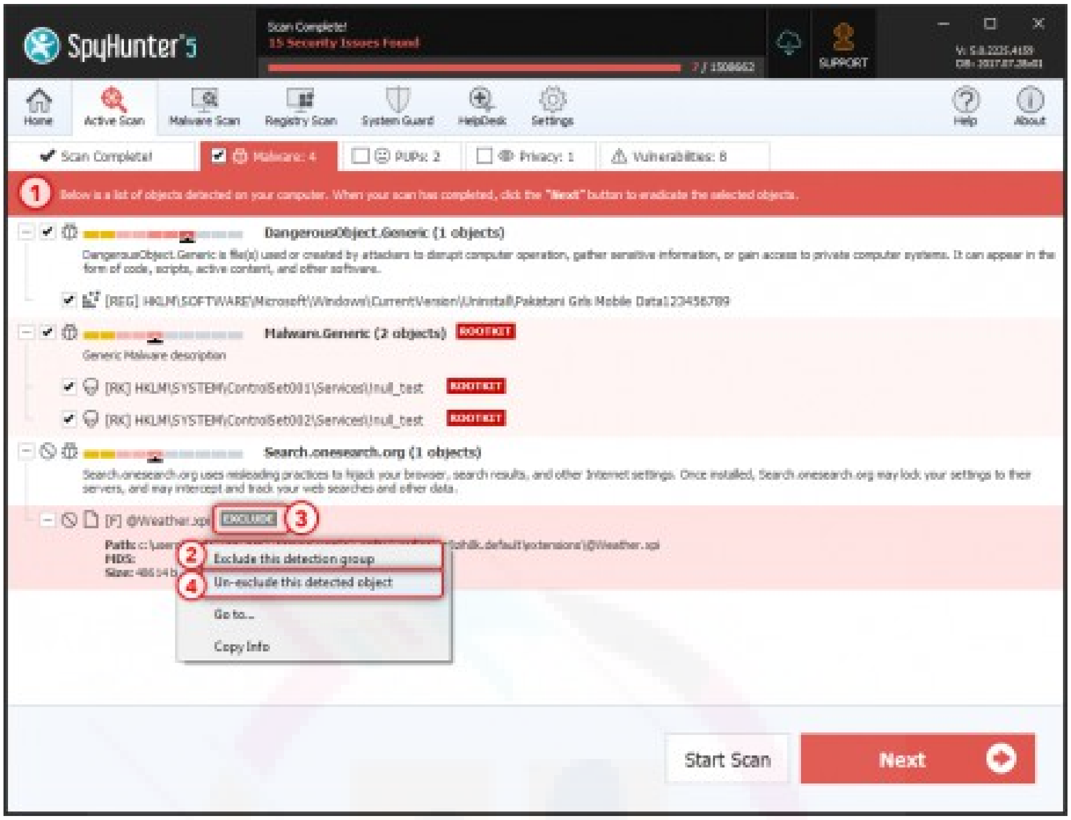
To select an object for removal, just select the checkbox at the left of the object. You can select or deselect any objects displayed in the "Malware," "PUPs" or "Privacy" tabs. We have included a convenient "Select All" feature that will allow you to select or deselect all objects displayed in a specific tab. To utilize this feature, simply select the checkbox at the left in the specific tab (9)

Once you have selected which objects you would like to remove, click the "Next " button.



Below is a list of malware objects detect
generally represents a security threat a
removed. Should you wish not to remov

Select Objects To Remove



Scan Complete!
15 Security Issues Found
7 / 1508662

V: 5.0.2225.4159
DB: 2017.07.28v01

1 Below is a list of objects detected on your computer. When your scan has completed, click the "Next" button to eradicate the selected objects.

DangerousObject.Generic (1 objects)

DangerousObject.Generic is file(s) used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software.

[REG] HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Pakistani Girls Mobile Data123456789

Malware.Generic (2 objects) ROOTKIT

Generic Malware description

[RK] HKLM\SYSTEM\ControlSet001\Services\null_test ROOTKIT

[RK] HKLM\SYSTEM\ControlSet002\Services\null_test ROOTKIT

Search.onesearch.org (1 objects)

Search.onesearch.org uses misleading practices to hijack your browser, search results, and other Internet settings. Once installed, Search.onesearch.org may lock your settings to their servers, and may intercept and track your web searches and other data.

[F] @Weather.xpi

Path: c:\user... ...fohlik.default\extensions\@Weather.xpi
MD5:
Size: 48654 b...

Press Next To Clean You PC

Note: Any objects that you choose to remove will be securely stored in SpyHunter's "Quarantine ." If, at any time, you would like to restore a previously removed object(s), you can do so through SpyHunter's "Restore " feature. To locate the object, go to the "Malware/PC Scan " tab and then click the "Quarantine " tab. From the "Quarantine " tab, you may restore an object by selecting the checkbox at the left of the object and clicking the "Restore " button.