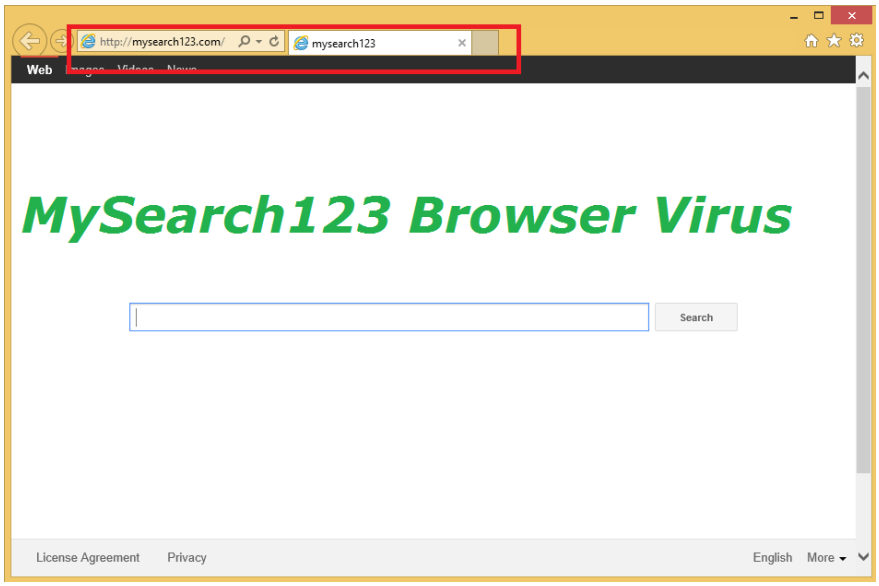
# Rooted MySearch123.com on Chrome, Firefox and Internet Explorer browsers

Technically MySearch123.com is not a virus that is classified as a malicious software program (unwanted program (PUP)) that can contain and install malicious programs on the computer. Your, like adware, toolbars or viruses.

MySearch123.com is one of the 'hijacker browser' that changes the default homepage and sets up the search "http://mysearch123.com/" in popular web browsers, such as Internet Explorer, Google Chrome or Firefox without user permission.

In the following article, Network Administrator will guide you through the steps to remove MySearch123.com from Internet Explorer, Google Chrome and Firefox browsers.




MySearch123.com is one of the 'hijacker browser' that changes the default homepage and sets up the search "http://mysearch123.com/" in popular web browsers, such as Internet Explorer, Google Chrome or Firefox without user permission.

In fact, MySearch123.com changed browser settings to redirect the browser to ads and make money.

MySearch123.com hijacker is designed to change your browser settings and can install additional plugins (toolbars, extensions - extensions or add-ons) on your web browser to promote links or other products.

Browser hijacker can redirect users' computers to malicious websites or install malicious programs, and cause security problems on the user's computer.

Technically "MySearch123.com" is not a virus that is classified as a malware program (unwanted program (PUP)) that can contain and install malicious programs on. Your computer, like adware, toolbars or viruses.

If a computer is the 'victim' of MySearch123 hijacker, then there will be lots of popup ads, banners and sponsored links (sponsored links) displayed on the screen or inside the Internet browser. And in some cases, computer speed may be 'slow' due to malicious programs running in the background.

MySearch123.com hijacker program can be installed without user notification.

The reason is because MySearch123.com is often 'packaged' within other free software that users download and install from unknown sites .

So when you install any program or software you need to pay attention to the program installation options, because most software installers contain additional software that you never want to install. put on your computer.

When installing a program on a computer:

1. On the installation screen, do not click the Next 'button too fast'.
2. Read carefully and accept the terms carefully.
3. Always select the 'Custom' setting.
4. Reject settings that require additional software that you do not want to install.
5. Uncheck any options saying that the homepage and search settings will be changed.

# Step 1: Remove MySearch123 with RogueKiller

RogueKiller is one of the programs against effective malware (malware). The program can detect, prevent and remove malware (malware) in general and both rootkits, rogues, worms, .

1. Download RogueKiller to your device and install it.

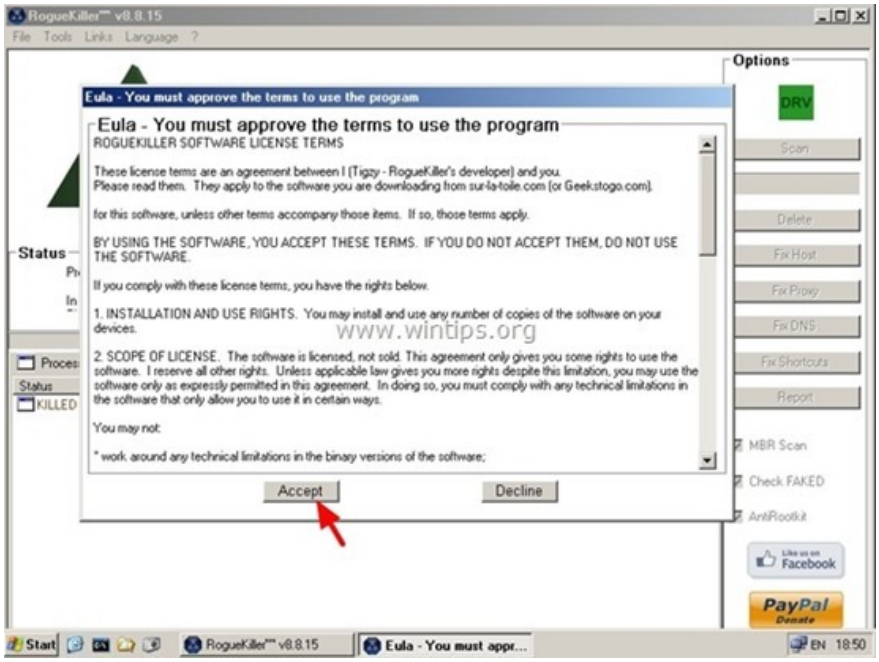
Download RogueKiller to your device and install it here.

**Note:**

Download the x86 or x64 version that matches your operating system version. To know the version of the operating system you are using, right-click the **Computer** icon, select **Properties** and search in the **System Type section** .

2. Double click to run RogueKiller.

3. Click **Accept** to agree to the terms, install the program.




4. The next step is to click **Scan** to scan for malware on your computer and on the startup port.


5. Finally, after the scan is complete, click the **Registry** tab, select all the items containing the malware found and click **Delete** to remove all the items.

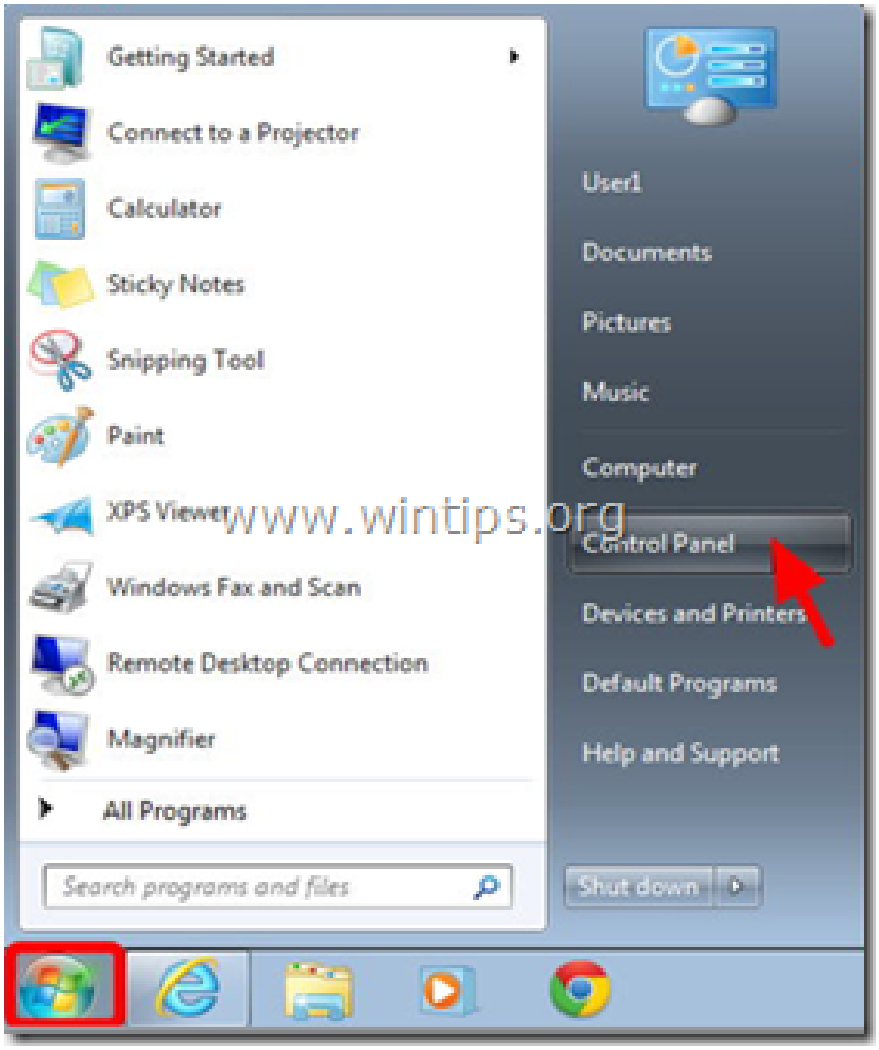

6. Close RogueKiller and proceed to the next step.

## Step 2: Uninstall malware MySearch123 from Control Panel

1. To do this, follow the steps below:

- On Windows 7 and Vista: **Start** => **Control Panel.**

- On Windows XP: **Start** => **Settings** => **Control Panel.**




- On Windows 8 and 8.1:

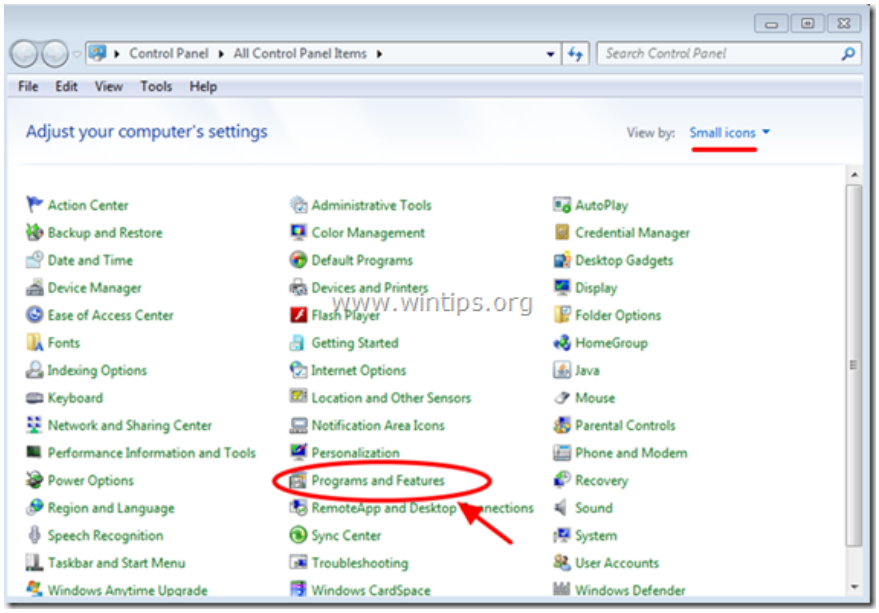
Press the **Windows + R** key combination to open the Run command window.

Enter **Control Panel** in the Run window and press **Enter.**

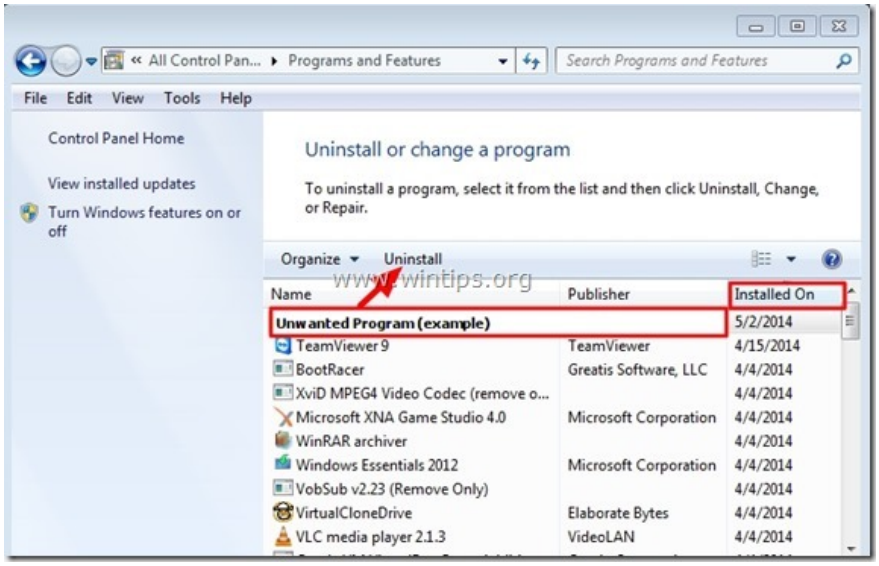
2. At the Control Panel window:

On Windows XP: select **Add or Remove Programs.**

On Windows 7, 8 or Vista: select **Programs and Features** (or Uninstall a Program).




3. In the next window, search for unknown programs in the installation section immediately, then proceed to uninstall those applications from the system.




Also find and remove malicious applications like:

1. MySearch123
2. MySearch123 New Tab
3. Go Mysearch123

4. GoSave
5. MuiTub

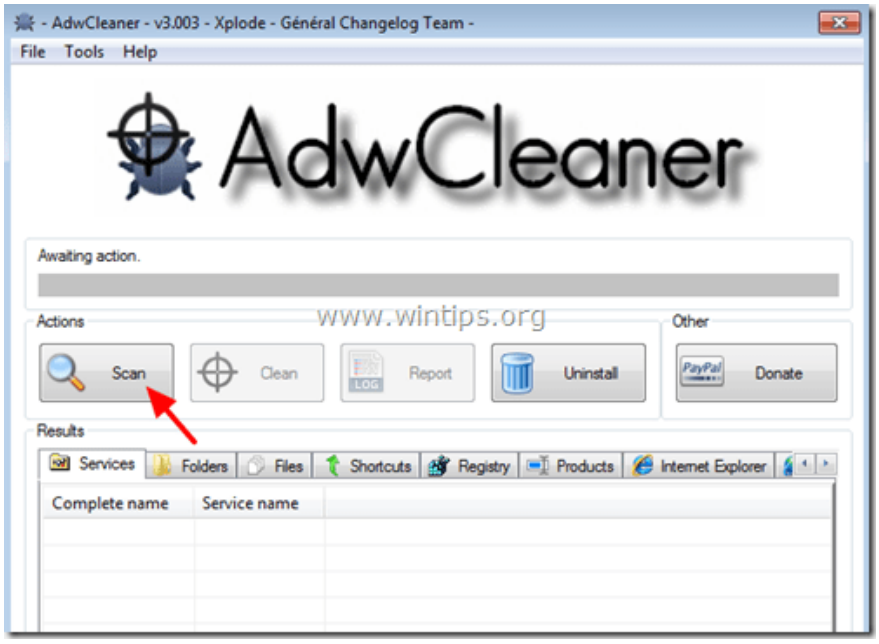
## Step 3: Remove MySearch123.com with AdwCleaner

1. Download AdwCleaner to your device and install it.

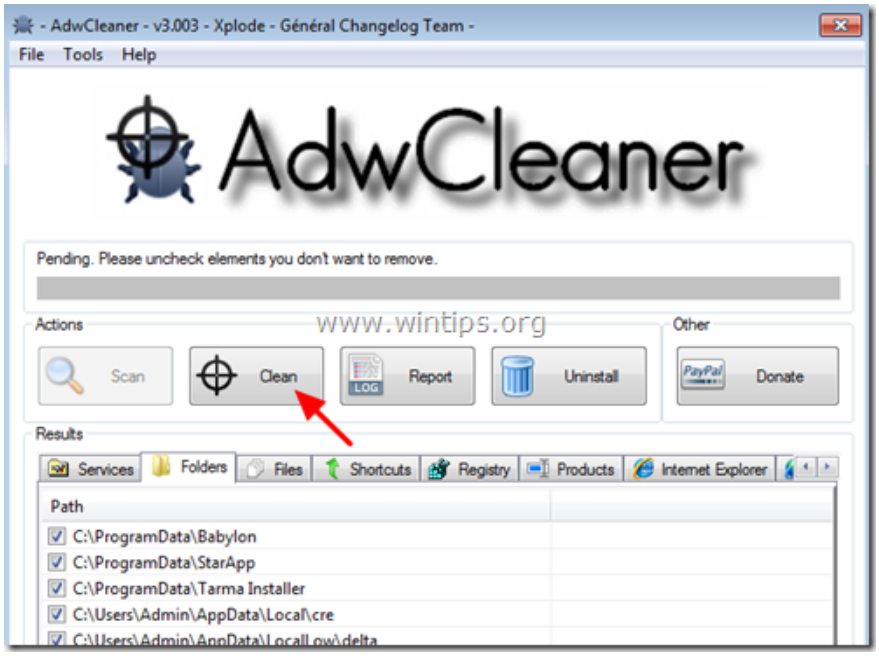
Download AdwCleaner to your device and install it here.

2. Close all open programs on your computer, then double click to open AdwCleaner.

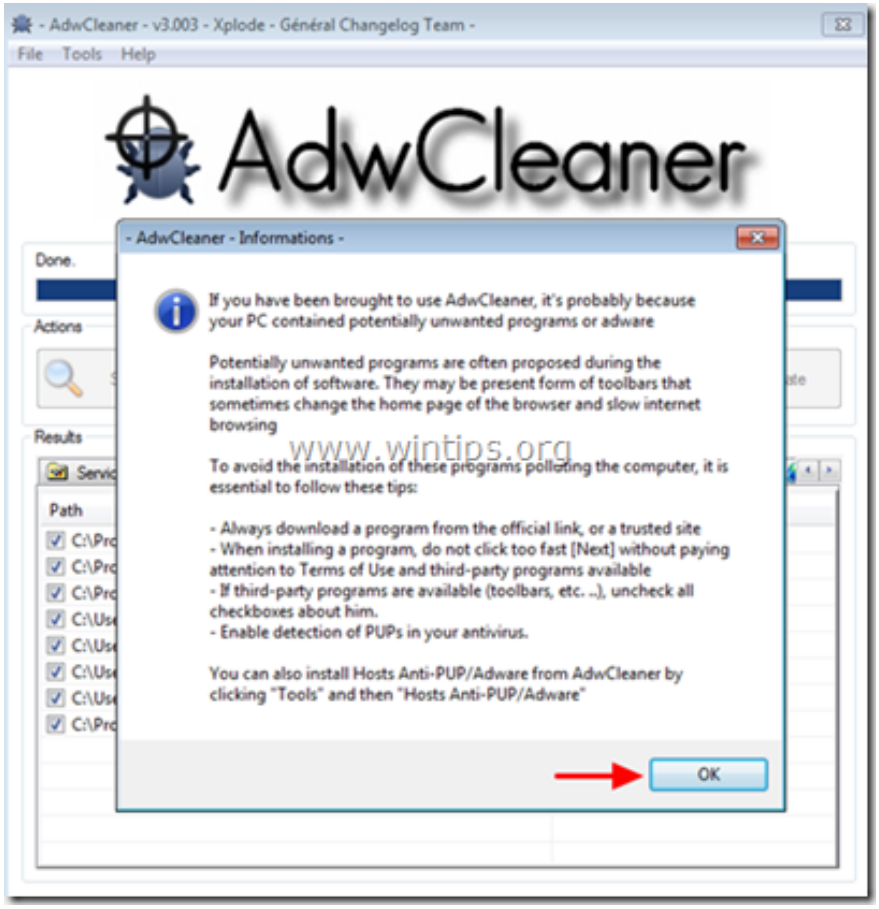
3. After accepting the terms, click the **Scan** button **.**




4. Wait until the scan has finished, click **Clean** to remove all unwanted malware on your system.



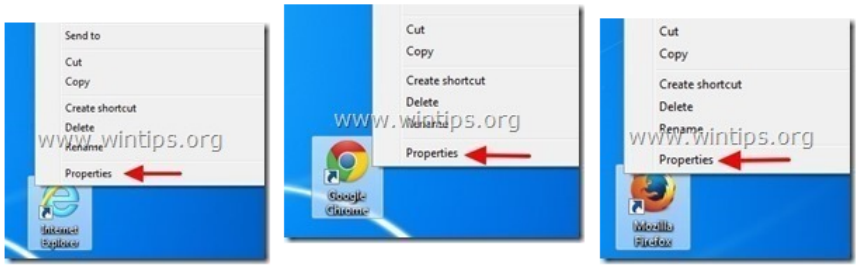

5. On the AdwCleaner - Information window, click **OK** , then select **OK** again to restart your computer.




5. When your computer is restarted, close the AdwCleaner "window" and proceed to the next step.

# Step 4: Uninstall MySearch123.com on Internet Explorer shortcut

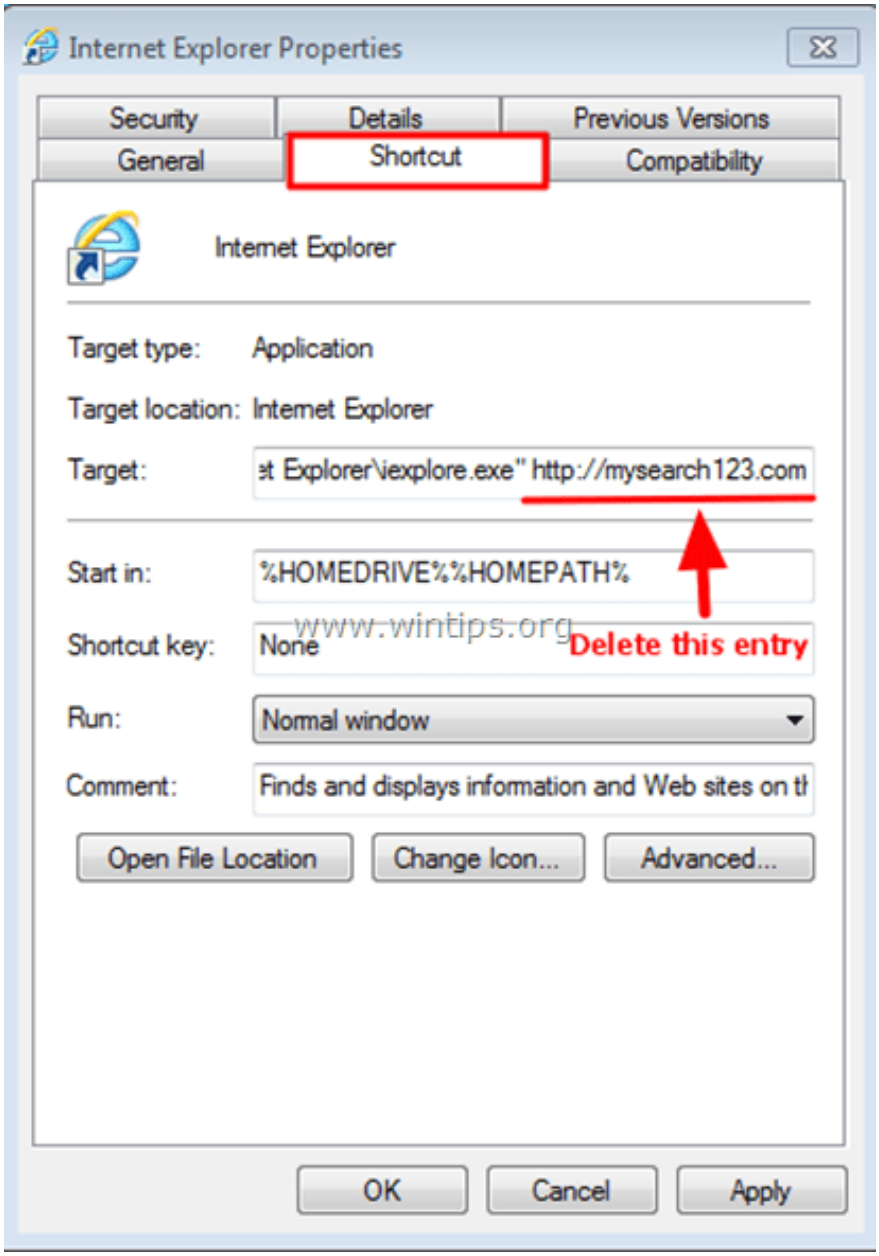
1. Right-click the Internet Explorer browser icon, then select **Properties** .




**Note:**

You must follow the same steps on all Internet Explorer browser shortcuts, including the Program lits list and the Taskbar.

2. At the Shortcut tab, find the Target pane and delete **MySearch123** (such as http:///mysearch123.com .) that comes with iexplore.exe (with IE shortcut) or firefox.exe (Firefox browser shortcut) or chrome.exe (for Chrome browser shortcut), then select **OK** .




If you receive a notice of 'Provide administrator permission to change these settings', click **Continue.**

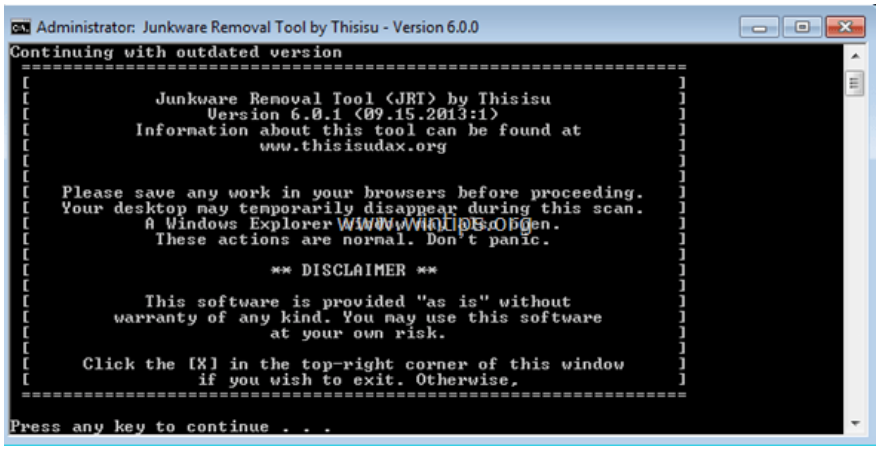
3. Follow the next steps.

## Step 5: Remove the Junkware MySearch123.com file using the Junkware Removal Tool

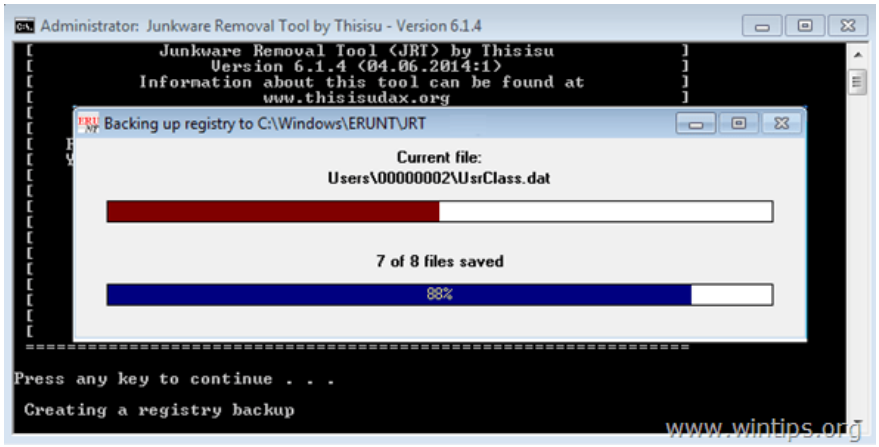
1. Download the Junkware Removal Tool on your device and run the tool.

Download the Junkware Removal Tool on your device and install it here.

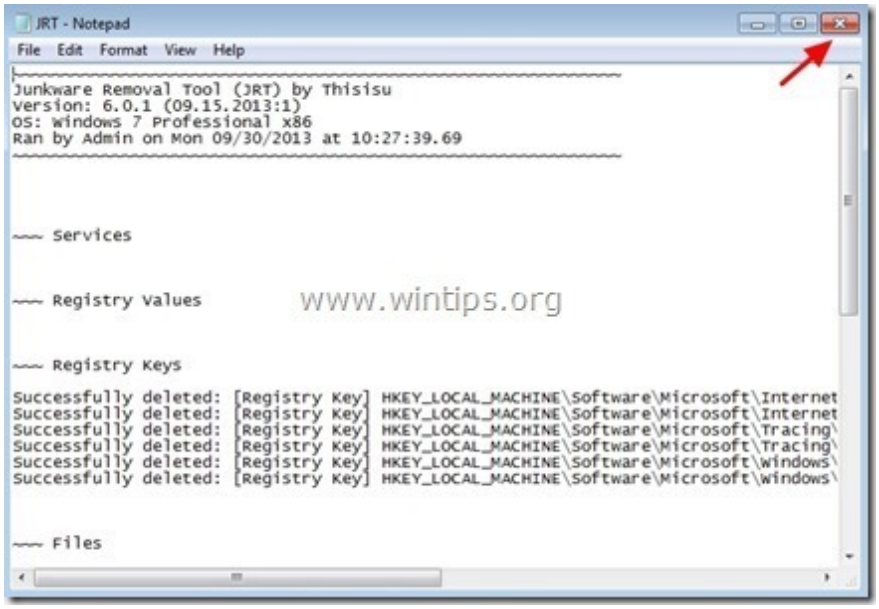
2. Press any key to start scanning your computer using the JRT - Junkware Removal Tool.




3. Wait until the JRT - Junkware Removal Tool scans and "cleans" your system.




4. Close the JRT window and restart your computer.




## Step 6: Remove MySearch123.com malware by Malwarebytes Anti-Malware

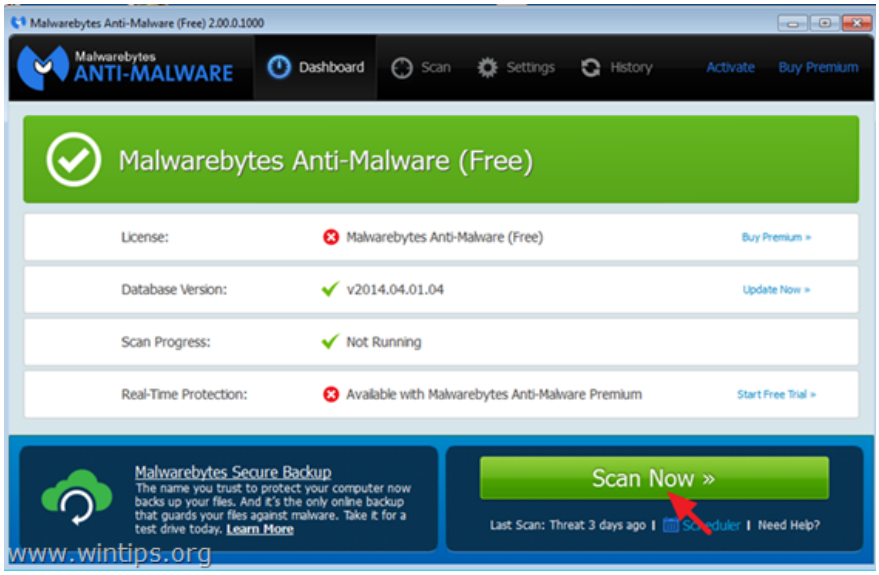
Download Malwarebytes Anti-Malware Premium to your device and install it.

Download Malwarebytes Anti-Malware Premium to your computer and install it here.

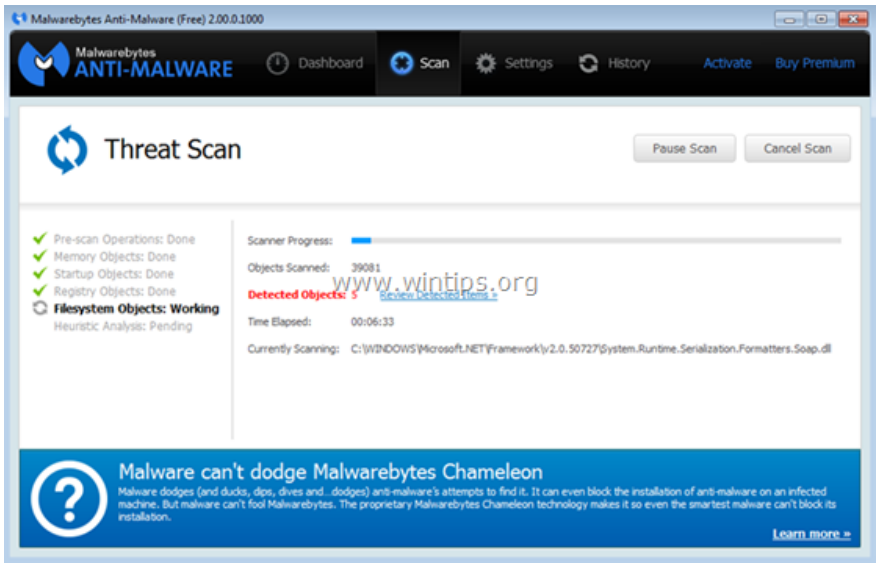
Scan and clean your computer with Malwarebytes Anti-Malware:

1. Run Malwarebytes Anti-Malware and allow the program to update (update) the latest version (if needed).

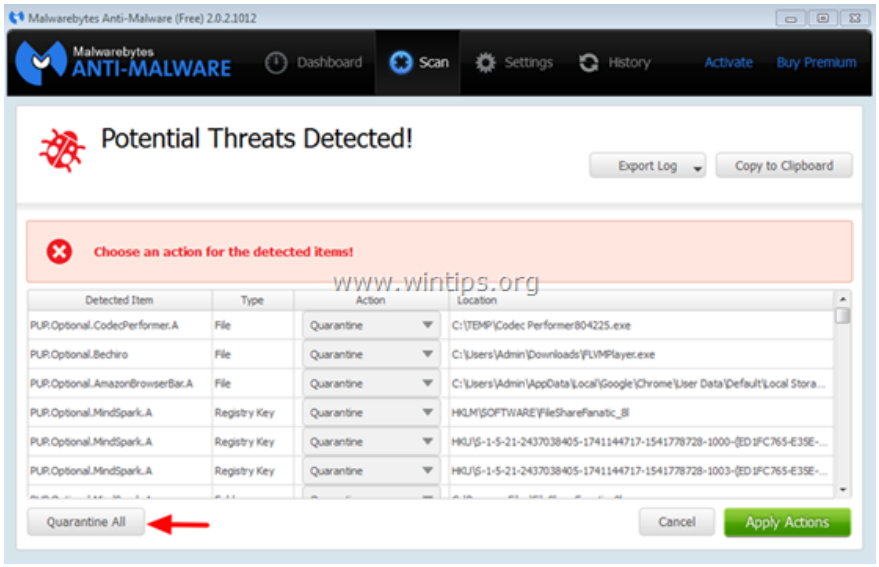

2. After the update process finishes, click the **Scan Now** button to start the scan of your system, remove malware and unwanted programs.



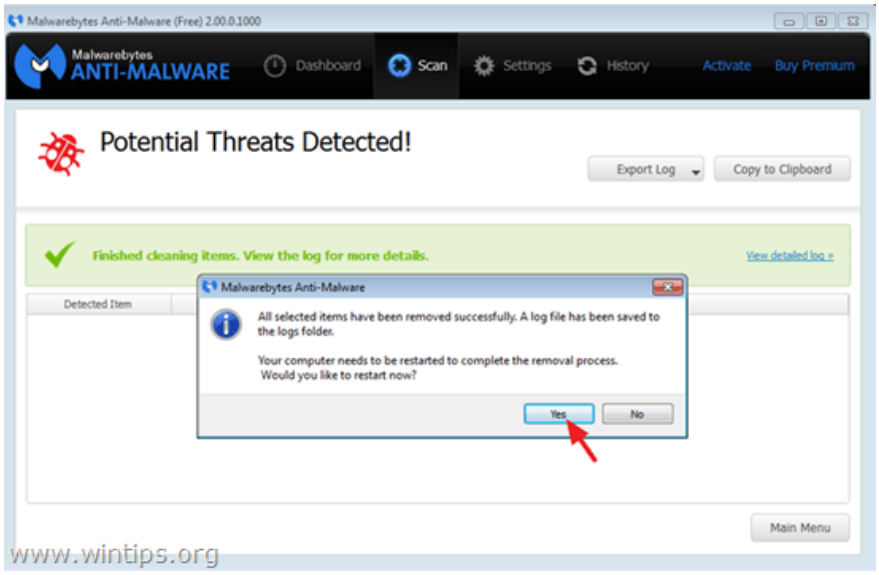

3. Wait until the system scan finishes.




4. Click the **Quarantine All** button to remove all "threats" found on your system.




5. After the process has finished, restart your computer to complete the process.

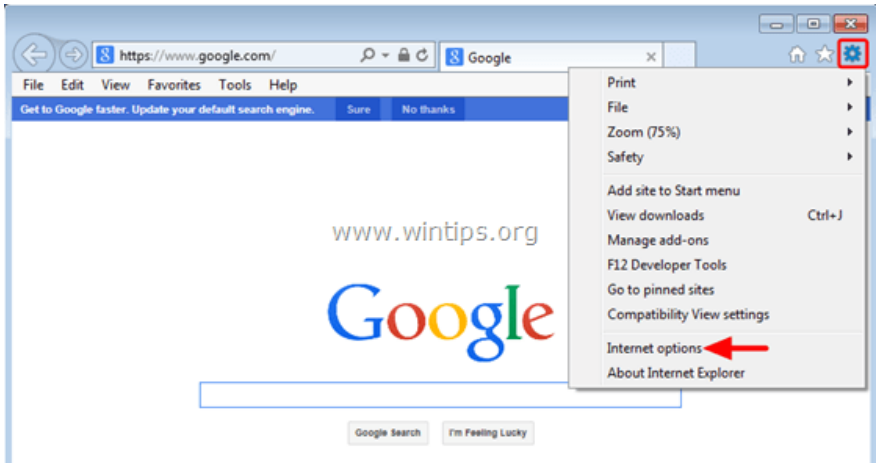



6. After the computer has finished booting, run Malwarebytes' Anti-Malware again to confirm there are no "threats" on your system.

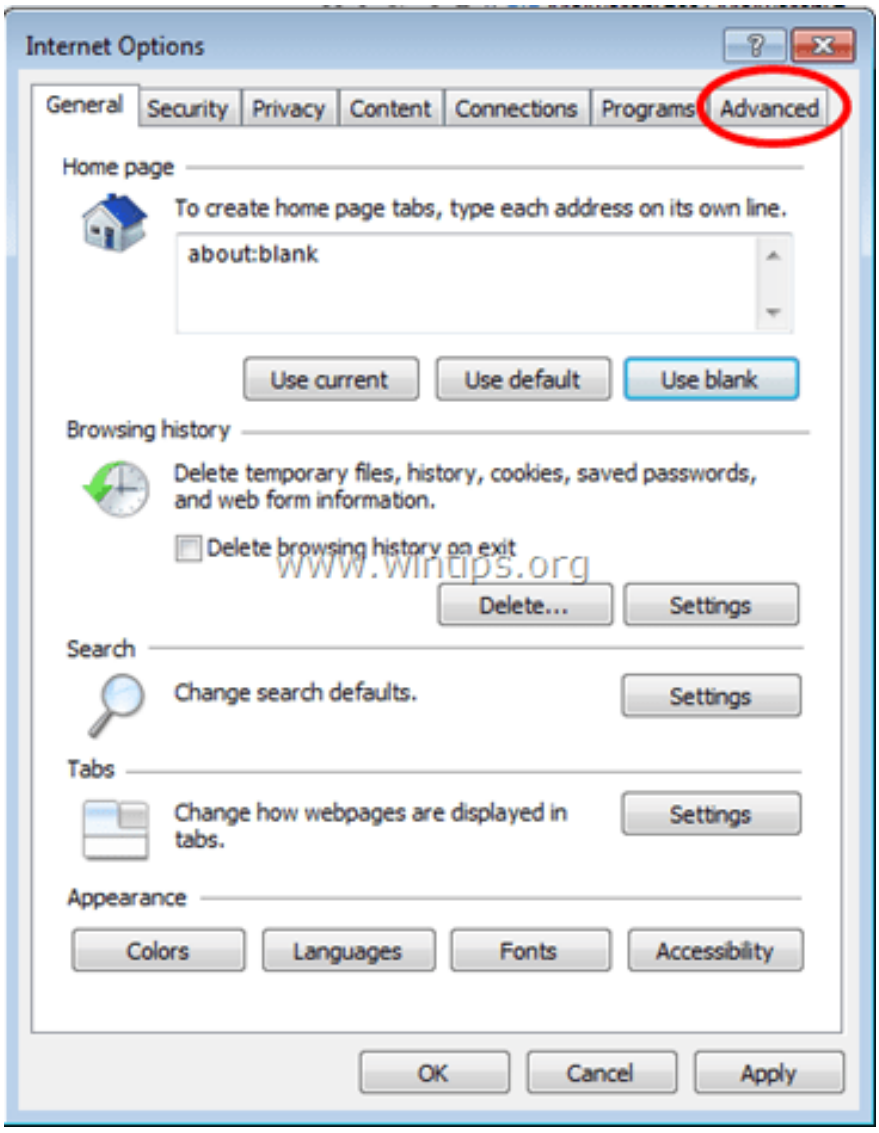
# Step 7: Uninstall MySearch123.com from Internet Explorer, Chrome and Firefox browsers

### - Internet Explorer browser:

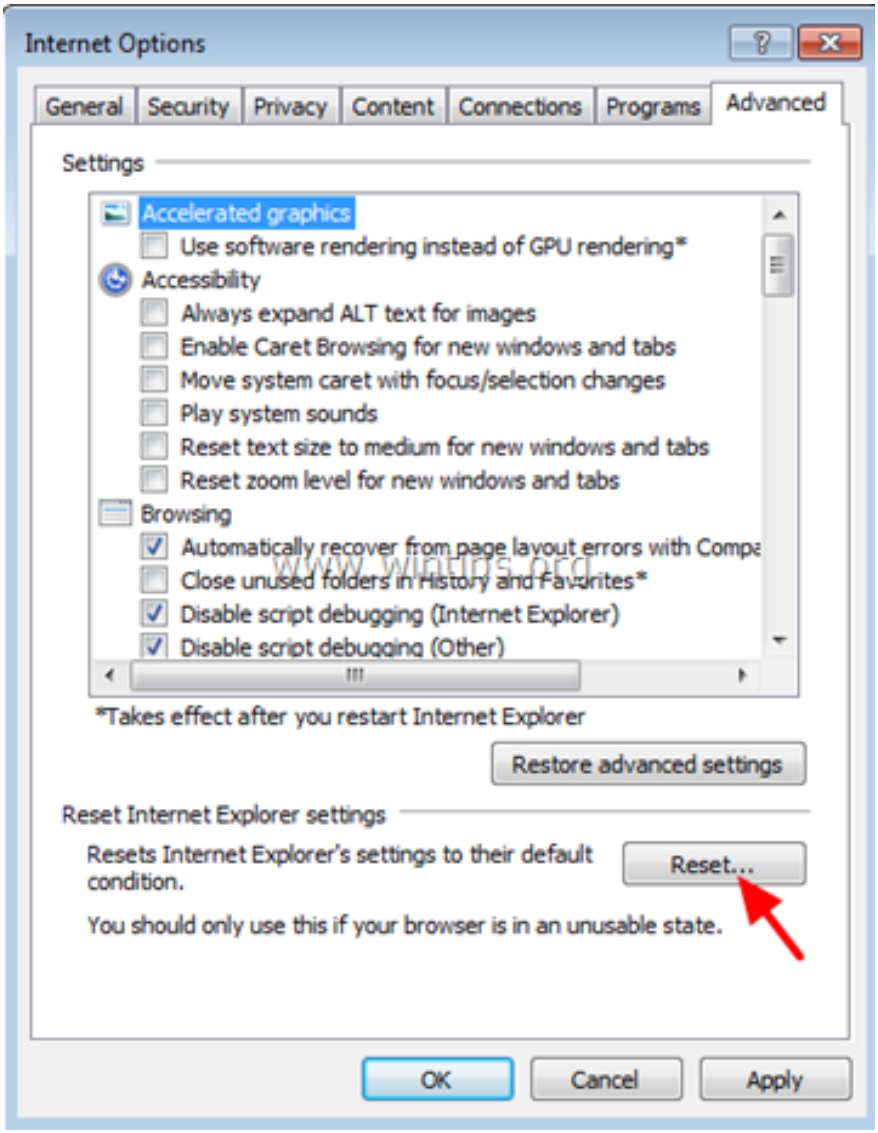
1. In Internet Explorer, select the jagged icon in the top right corner, select **Internet Options** .



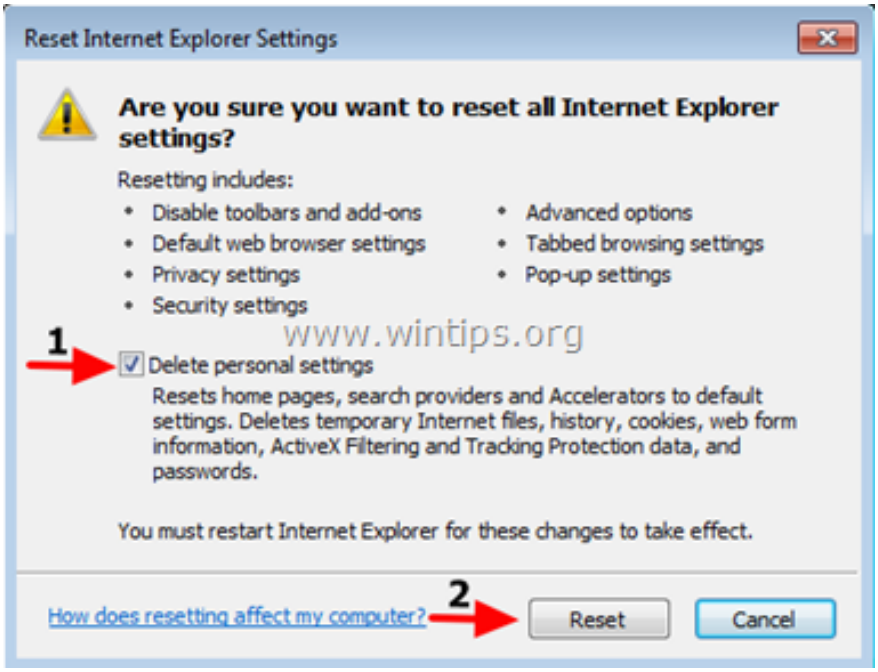

2. Next click on the **Advanced** tab **.**



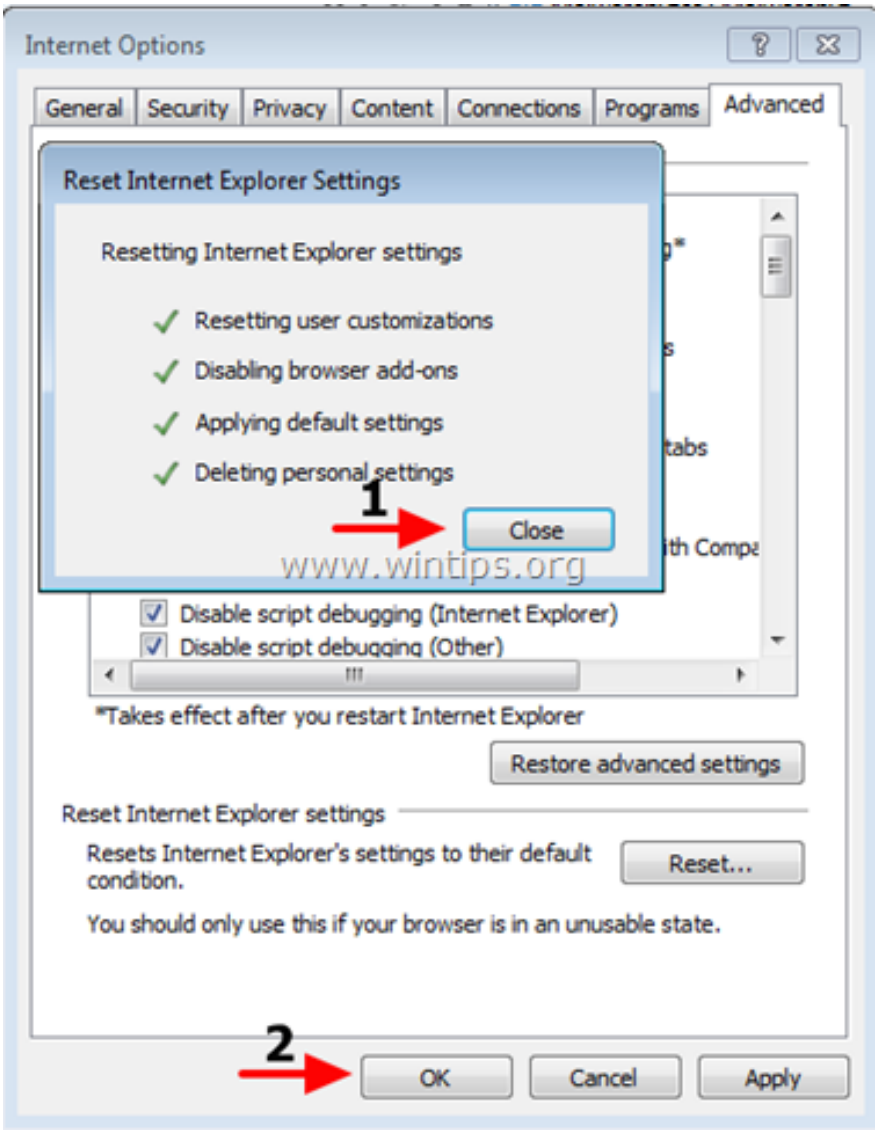

3. Select **Reset** .




4. Check the **Delete personal settings** option then click **Reset** .



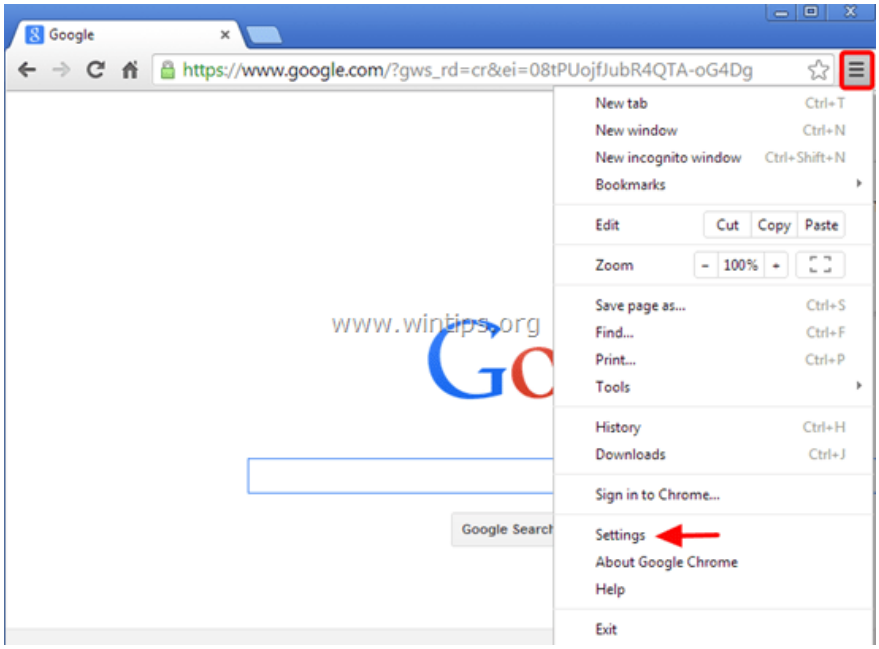

5. After the reset process ends, click **Close** then click **OK** to exit the Internet Options window.



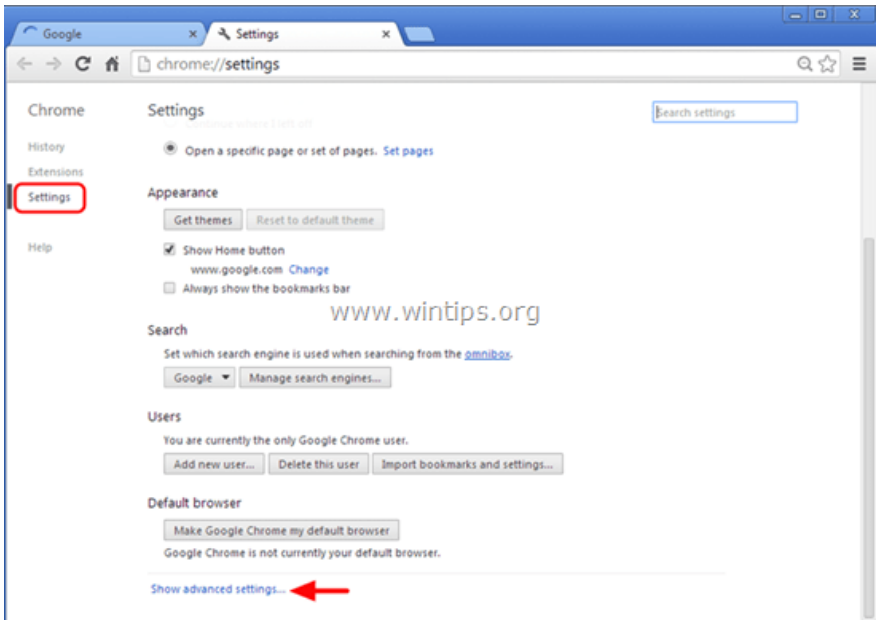

6. Close all windows and then restart Internet Explorer.

## - On Chrome browser:

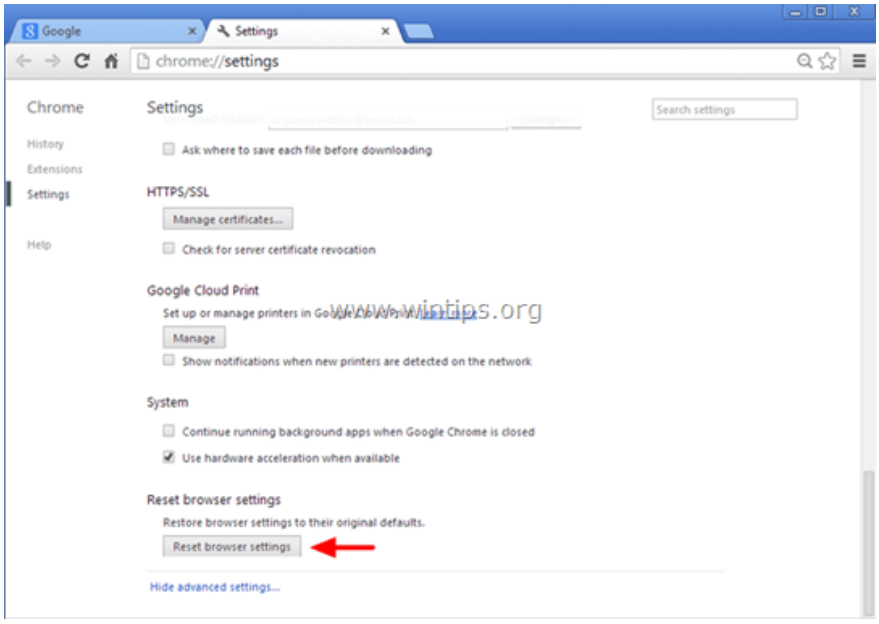
1. Open the Chrome browser on your computer, then click the 3 dash icon icon in the top right corner of the screen, select **Settings** .



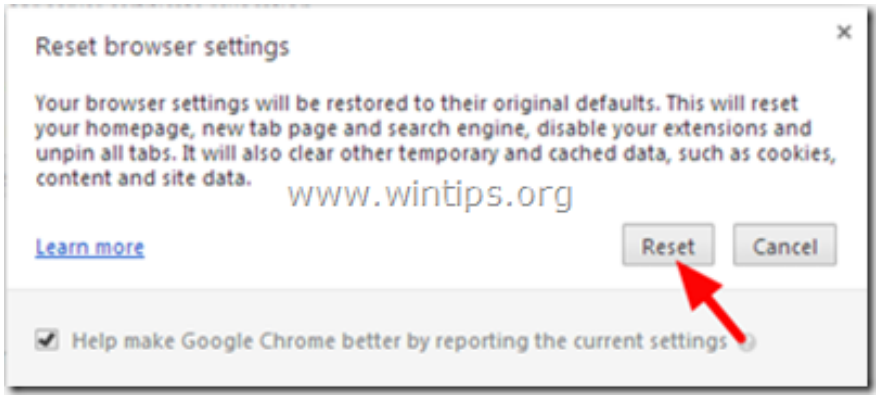

2. On the Settings window, find and click the option **Show advanced settings** (show **advanced settings** ).




3. Scroll down to find and select **Reset Browser Settings** button.



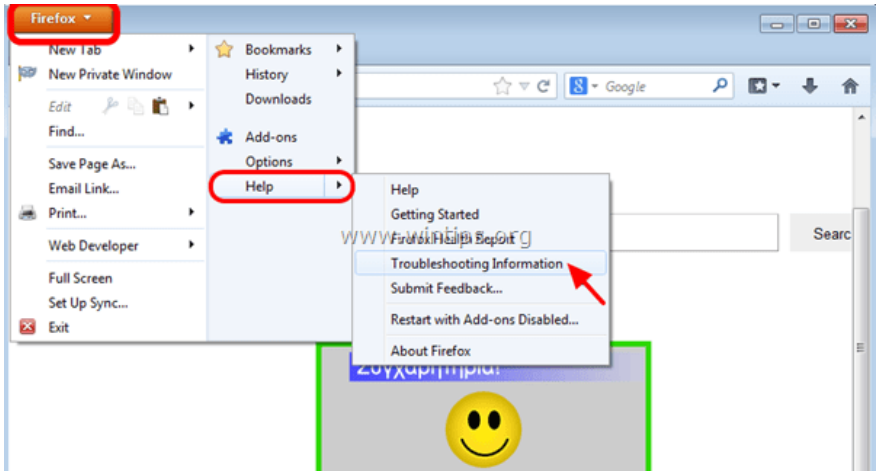

4. In the Reset browser settings dialog window, click **Reset** .



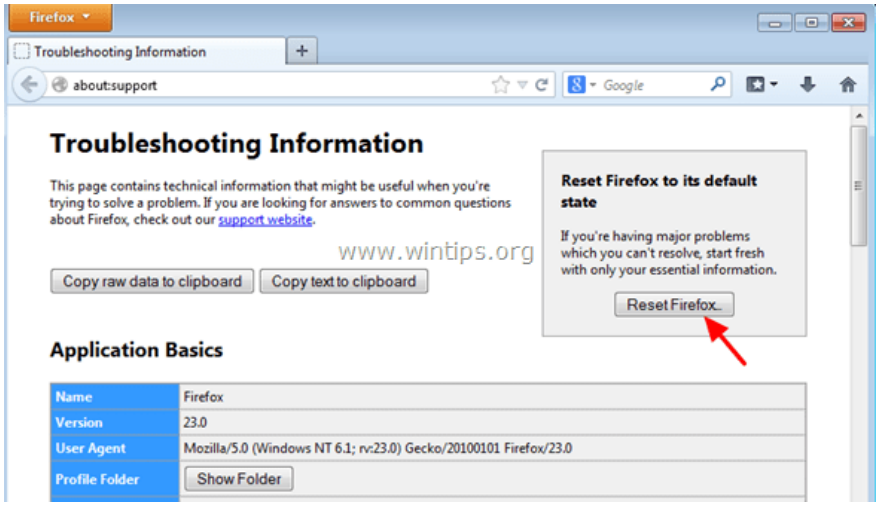

5. Restart your Chrome browser.

## - Mozilla Firefox browser:

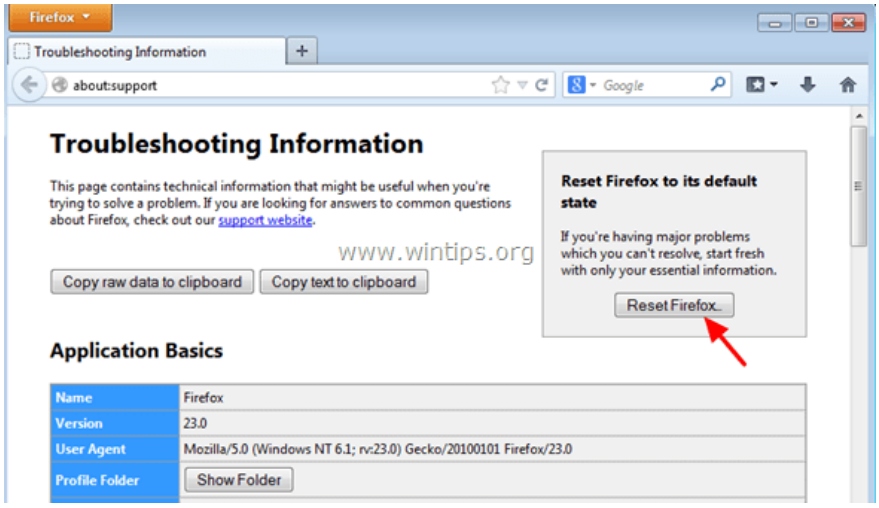
1. On the Firefox Menu, access **Help** => **Troubleshooting information** .




2. Next to the Troubleshooting Information window, click the **Reset Firefox** button to reset Firefox to its original default state.




3. Click **Reset Firefox** again.



4. After the reset process finishes, restart your Firefox browser.

## Refer to some of the following articles:

1. Summary of 10 ways to fix Not Responding errors on Chrome browser
1. Trick 'tail-cutting' Google, Facebook and Apple
1. Instructions for fixing errors without network connection on Chrome browser

**Good luck!**