How to Get Rid of Snap Do

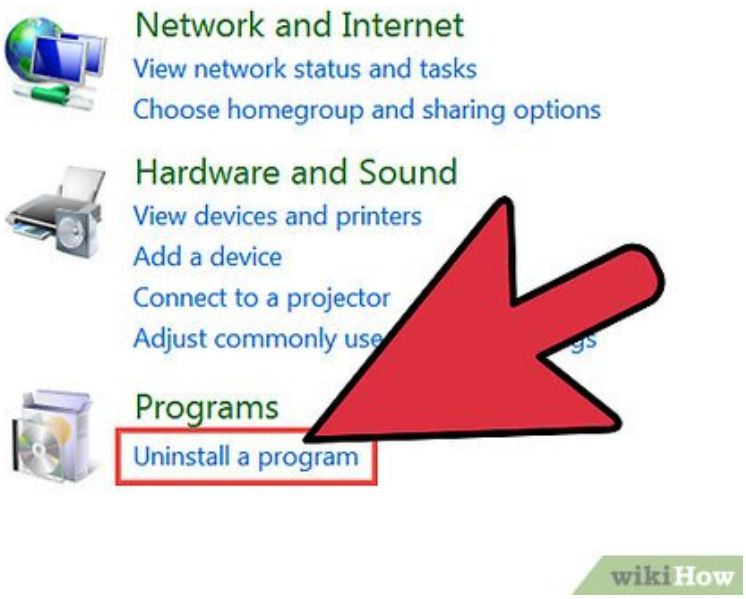
Snap Do is a custom search engine and toolbar program that may have been installed at the same time you downloaded a separate third-party application to your computer, such as vShare. Applications such as Snap Do are commonly referred to...

Part 1 of 4:

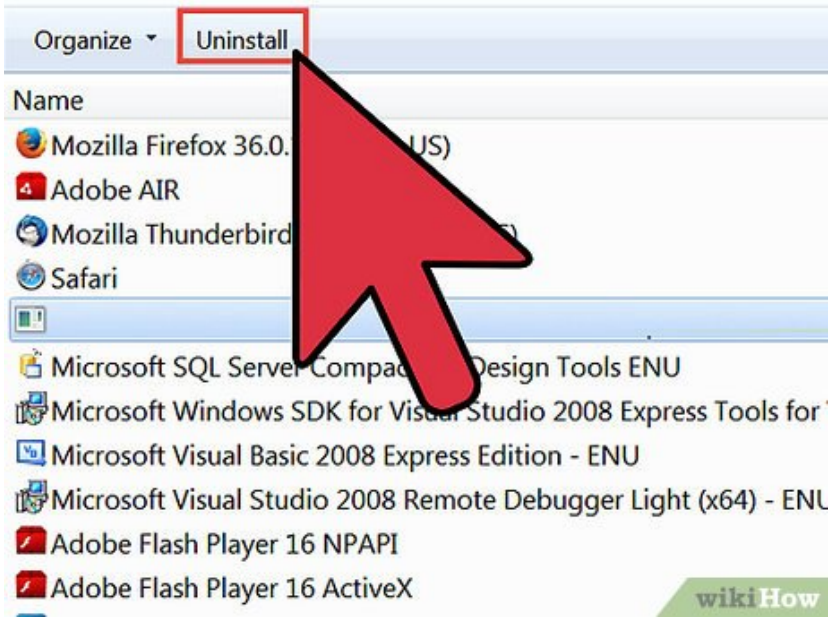
Uninstalling Snap.Do Software

1. 

Open the Control Panel. You can access this from the Start menu. Windows 8 users can press ? Win and type "control panel".

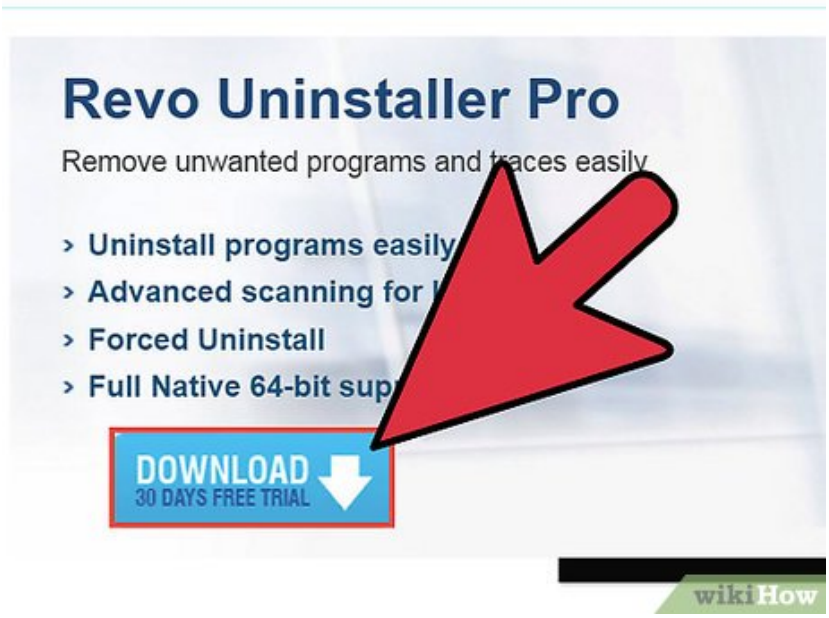
2. 

Select "Programs and Features". If you are in Category View, select "Uninstall a program".

3. 

Find and delete any Snap.Do entries. There are likely several programs on this list that will need to be deleted. Go through the list of installed programs, select the program you want to remove, and click the Uninstall button to delete each one:

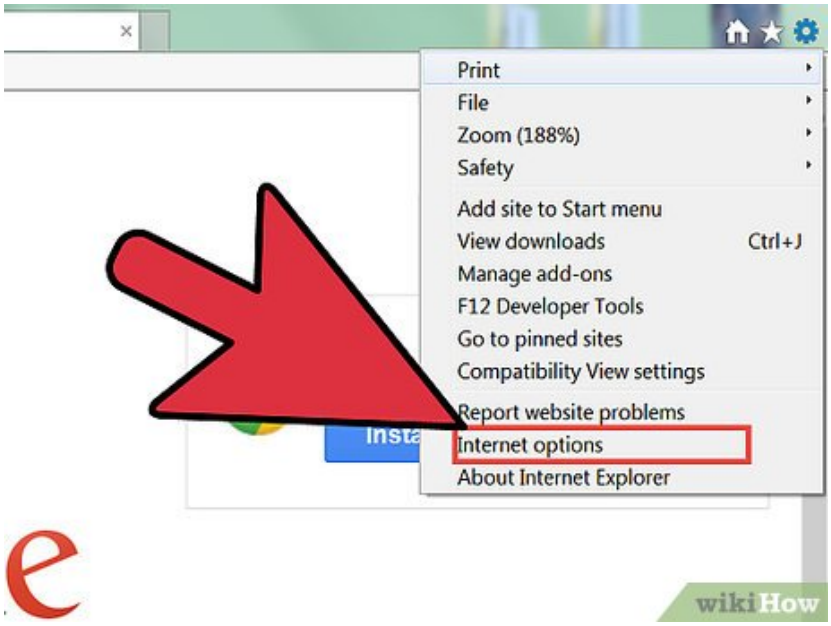
1. SnapDo toolbar
2. Snap.Do Updater
3. Shopping Helper Smartbar
4. Shopping Helper Smartbar Engine
5. Saving Expert Smartbar
6. Any other programs published by ReSoft Ltd.

4. 

Use Revo Uninstaller for tricky programs. If any of the programs in the list will not allow you to remove them, you can use Revo Uninstaller to get rid of them. Click here for detailed instructions.

Part 2 of 4:

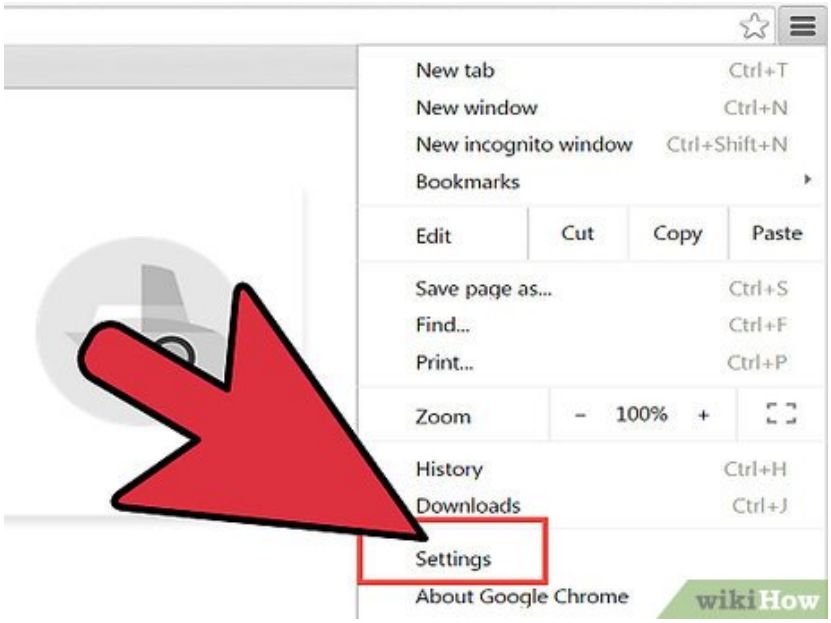
Resetting Your Browsers

1. 

Reset Internet Explorer. Even if you don't use Internet Explorer on a regular basis, you'll still need to reset it as it is used for some Windows functions.

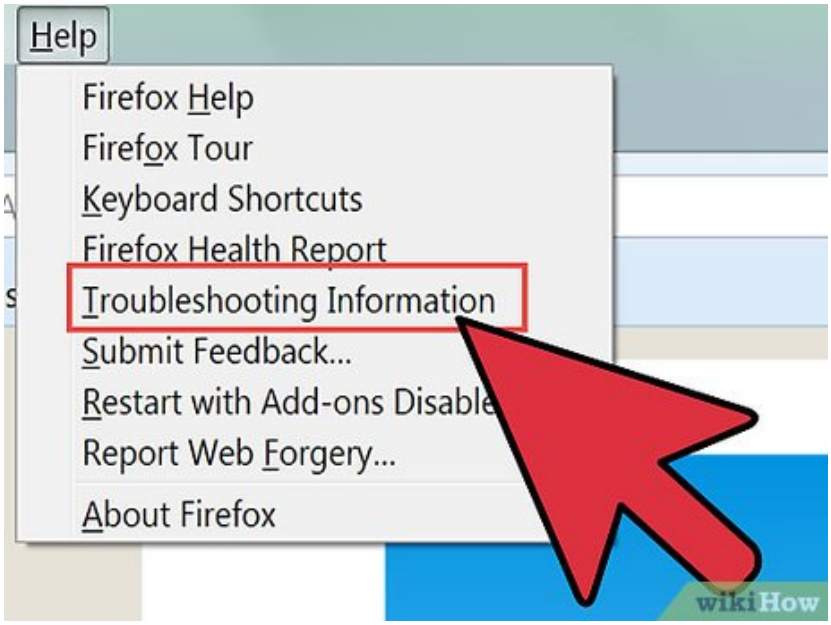
1. Open Internet Explorer.
2. Click the Gear icon or the Tools menu.
3. Select "Internet options".

4. Click the Advanced tab and then the Reset... button.
5. Check the "Delete personal settings" box and click Reset.

2. 

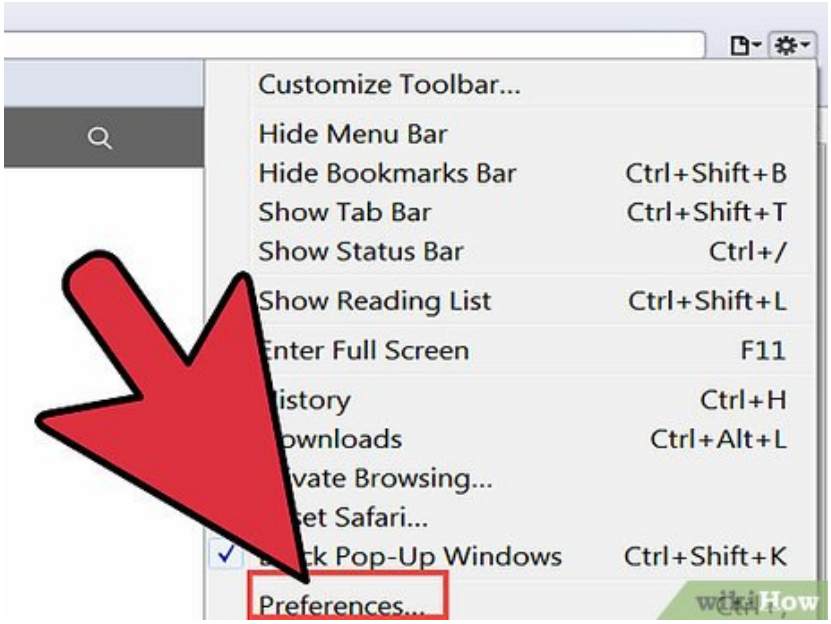
Reset Chrome (if installed). If you use Google Chrome for web browsing, you'll want to reset it to delete any Snap.Do toolbar software. If you don't use Google Chrome, skip down to the next step.

1. Open Google Chrome.
2. Click the Chrome Menu button (?).
3. Select "Settings".
4. Click the "Show advanced settings..." link.
5. Scroll to the bottom and click Reset settings.
6. Click Reset to confirm.

3. 

Reset Firefox (if installed). If you use Firefox for web browsing, you'll want to reset it to delete any Snap.Do toolbar software. If you don't use Firefox, skip down to the next step.

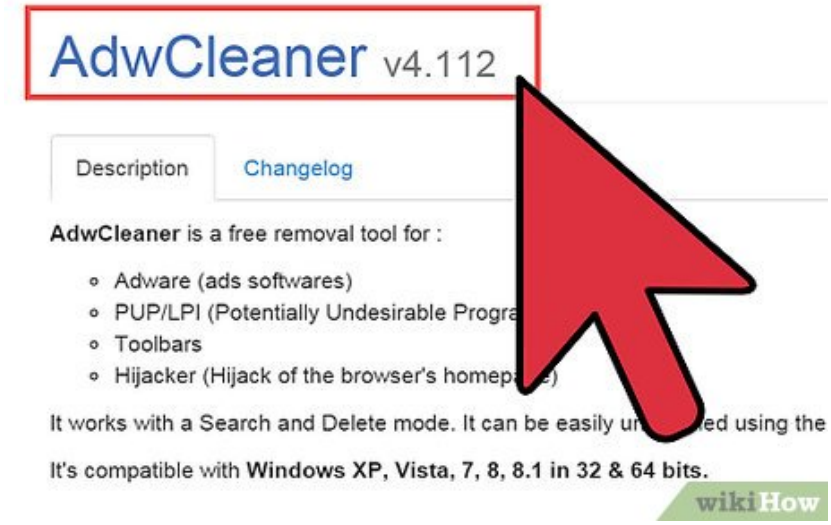
1. Open Firefox.
2. Click the Firefox Menu button (?).
3. Click the Help (?) button then click "Troubleshooting information".
4. Click Reset Firefox... and then Reset Firefox to confirm.

4. 

Reset your other browsers. If you use any other browsers such as Opera or Safari, reset them as well. Snap.Do will likely infect all of the browsers installed on your computer, so make sure to reset each one you.

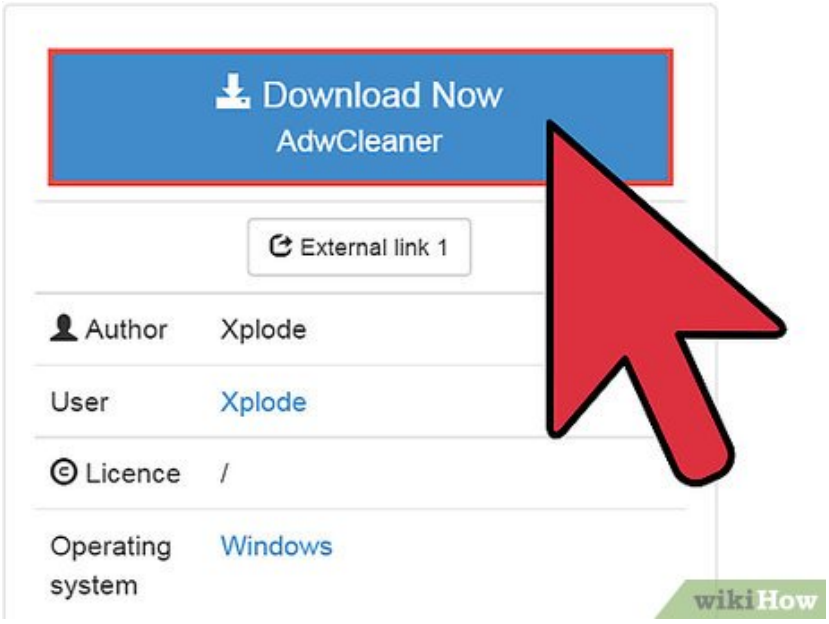
Part 3 of 4:

Removing Lingering Snap.Do Software

1. 

Download your tools. Once you've uninstalled the software and reset your browsers, Snap.Do will still be on your system. You'll need the help of some tools in order to completely eradicate it. All of these tools are available for free:

1. AdwCleaner - `general-changelog-team.fr/en/tools/15-adwcleaner`
2. Malwarebytes Antimalware - `malwarebytes.org`
3. HitmanPro - `surfright.nl/en/hitmanpro`

2. 

Install and run AdwCleaner. Follow the prompts to install the program, and then click the "Scan" button once you open it. AdwCleaner will scan your computer for infections and report them when its finished.

1. Click the "Clean" button once the scan is complete to remove any infections that AdwCleaner finds.

3. 

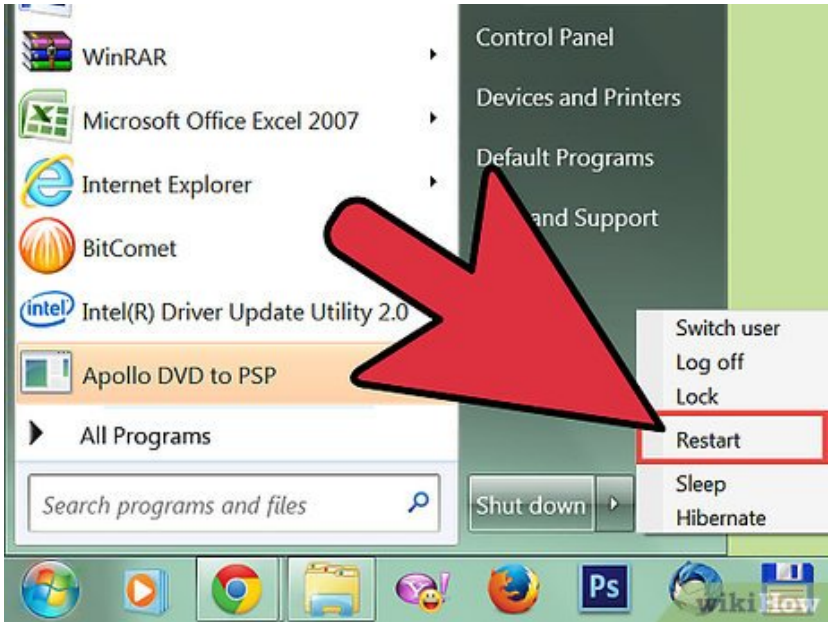
Install and run Malwarebytes Antimalware.Make sure to update the program after installing it to ensure that you have all the latest detections.

1. Click the "Scan Now" button to run an Antimalware scan. This will likely take about 30 minutes to an hour.
2. After the scan is finished, click the "Quarantine All" button and then click "Apply Actions".
3. Reboot your computer after quarantining the detected files.

4. 

Install and run HitmanPro. During installation, uncheck the option that allows HitmanPro to scan your system every time it boots up. Leaving this enabled will slow down your system unnecessarily.

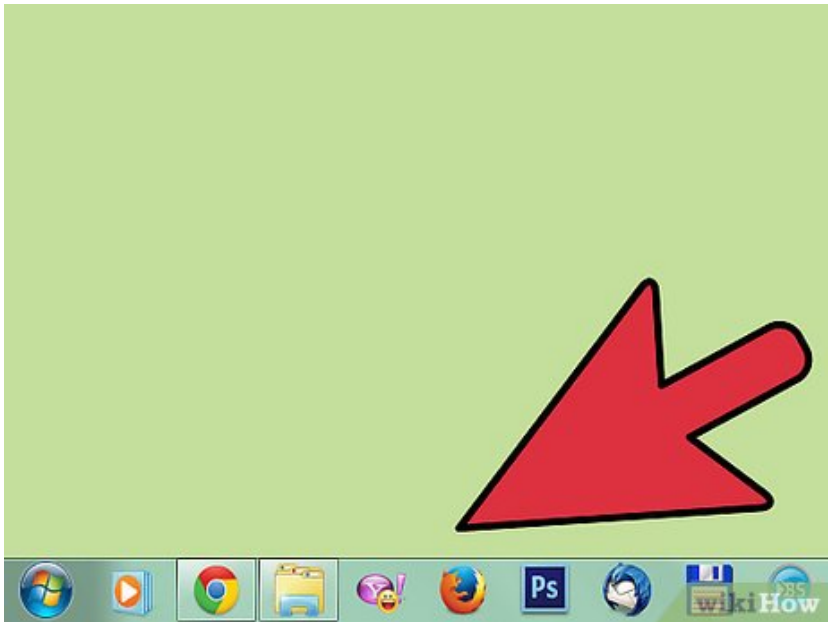
1. HitmanPro will begin scanning as soon as installation is complete. Click the "Activate free license" button after reviewing the scan results to deleted the selected infections.

5. 

Reboot your computer and run each antimalware scan again. Occasionally some pieces of Snap.Do will slip through the cracks and show up again after the computer has rebooted. To ensure that your computer is completely free of infections, reboot your computer and run each of the scans above again.[1]

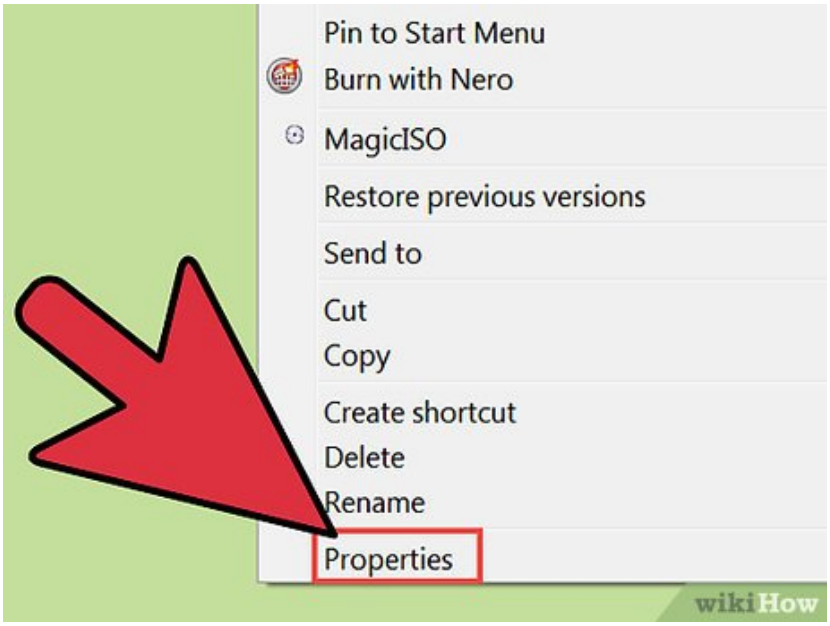
Part 4 of 4:

Fixing Your Browser Shortcuts

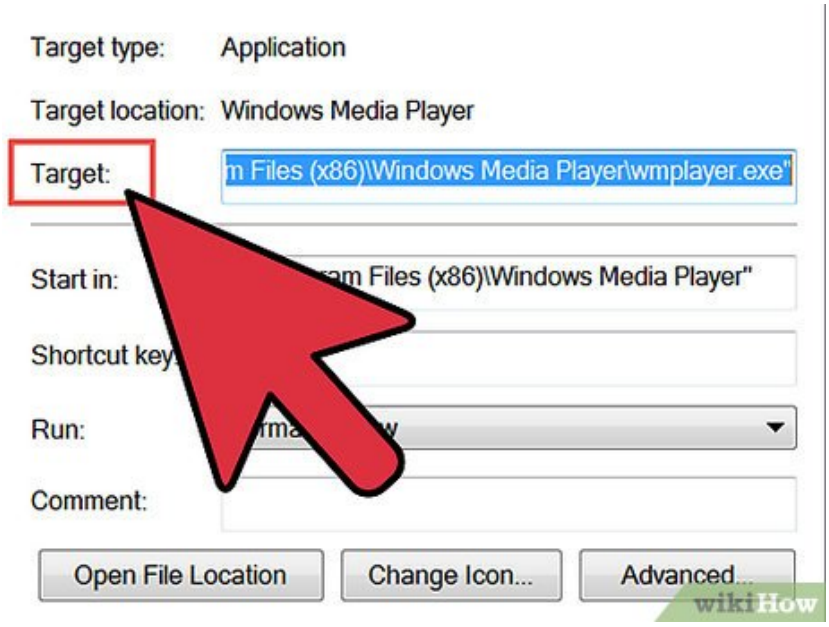
1. 

Track down all of your browser shortcuts. Snap.Do may make changes to each of your internet browser shortcuts which will make them automatically direct you to the Snap.Do homepage. Fixing these shortcuts will prevent you from getting re-infected.

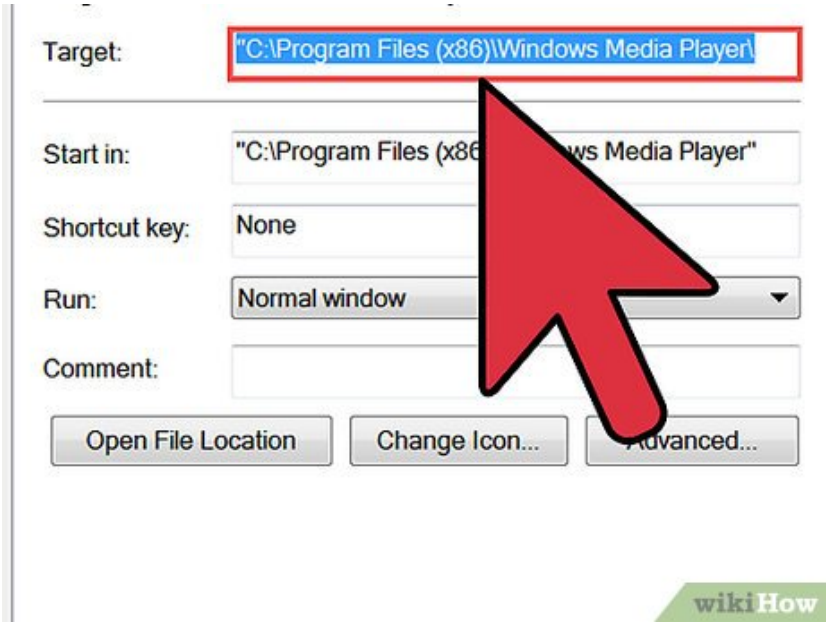
1. You likely have shortcuts located in several different places, and all of them will need to be changed one-by-one. Common locations include: Desktop, Start menu, Taskbar, and the Quick Launch bar.

2. 

Right-click on the shortcut and select "Properties".

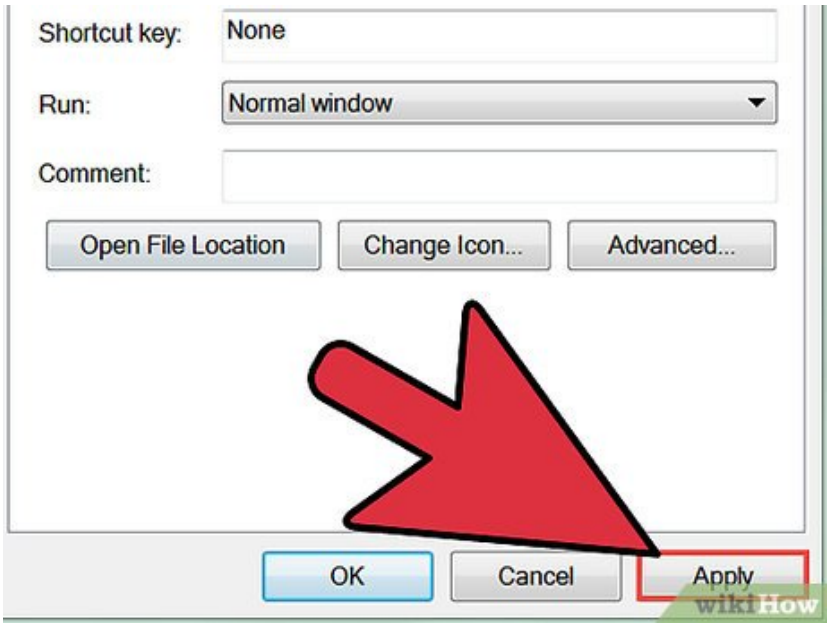
3. 

Locate the "Target" filed. This can be found in the Shortcut tab.

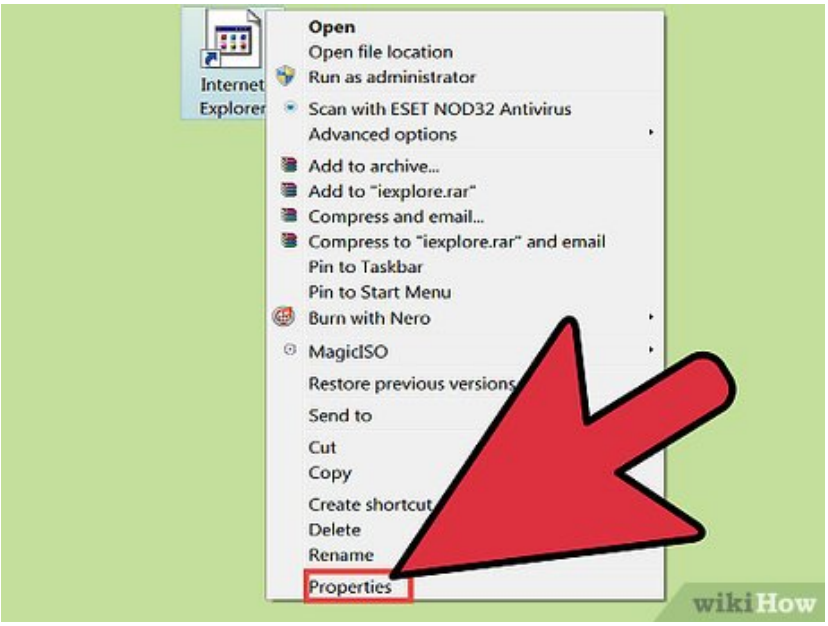
4. 

Find the URl at the end of the Target shortcut. For example, the Internet Explorer Target may be shown as `"C:Program FilesInternet Exploreriexplore.exe""www.Snap.do"`. Remove the `www.Snap.do"` from the end of the line.

1. You may not have anything at the end of the shortcut, which means one of the antimalware scanners already took care of the problem. You should still double-check every shortcut.

5. 

Click Apply **to save your changes.**

6. 

Repeat this for every browser shortcut on your computer. Make sure that you double-check every browser, as forgetting one can lead to all of your work being undone when you accidentally open it.[2]

You finished reading the article "**How to Get Rid of Snap Do**" 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.

© 2019 TipsMake.com