Completely remove Adware and Spyware on your system

Adware is a pop-up ad displayed on a computer or on an advertisement. Spyware is a program that controls activities and information on your computer, then sends this information to another remote computer.

Adware is a pop-up ad displayed on a computer or on an advertisement. Spyware is a program that controls activities and information on your computer, then sends this information to another remote computer.

Both Adware and Spyware are dangerous programs. Once your computer is infected with Adware and Spyware, they will start to attack and destroy your system. So how to completely remove Adware and Spyware on the system, please refer to the following article of Network Administrator.

If your computer is infected with malware, follow these steps to kill malware: Use Malwarebytes Anti-Malware Home to find, remove spyware, ads, malicious . on your computer.

1. Disconnect all Internet connections on the computer

Close all browser windows and applications on your computer (including email), then proceed to interrupt all Internet connections on your computer. The simplest way is to unplug the network cable that connects the computer to the modem or router.

2. Use the traditional application uninstall method

Some programs and applications installed on your computer may attach to both adware and spyware without your knowledge. So to "clean up" adware and spyware, the easiest way is to uninstall these programs. Before

proceeding to uninstall, open **Control Panel** => **Program** , then access the option **Uninstall or change a program** and check the programs installed on your computer.

If you find unwanted programs installed on your computer, you simply need to right-click the program's name and select **Uninstall to** finish.

On Windows Vista, access the **Programs and Features option** to remove applications and unwanted installation programs.

After removing Adware and Malware, restarting your computer is done.

3. Use an antivirus program to scan your computer

After disconnecting all Internet connections, removing adware and spyware and restarting your computer, the next step is to use antivirus programs to scan your entire system. If the antivirus program you are using allows, you can scan the entire system in Safe Mode. If you have not installed any antivirus program, you can choose to download and install paid antivirus programs or the best free antivirus programs to use.

4. Use SmitFraudFix, MalwareBytes, and other tools

Most spyware is distributed through Zlob family of Troijan downloader. SmitFraudFix is ??one of the best free tools to remove adware and spyware-related Zlob versions.

MalwareBytes supports the removal of scareware, the scam software that hijacks (hijackers) attacking your computer.

1. Download SmitFraudFix to your device and install it here.
2. Download MalwareBytes Anti-Malware to your computer and install it here.

5. Get access to the drive

Although scanning your entire system in Safe Mode is a good solution, it is not enough to prevent some malware. If adware and spyware still exist on your system even though you have applied everything and still can't get rid of them, the next solution you can Think of accessing the drive without the permission of adware

and spyware.

The best way to gain access to the drive is to use BartPE Bootable CD. After starting BartPE CD, you can access File manager (file manager), find the antivirus programs you install and scan your system again. Or locate files and folders as 'culprits' and proceed to delete those files and folders.

6. Undo the Residual Damage (indirect damage)

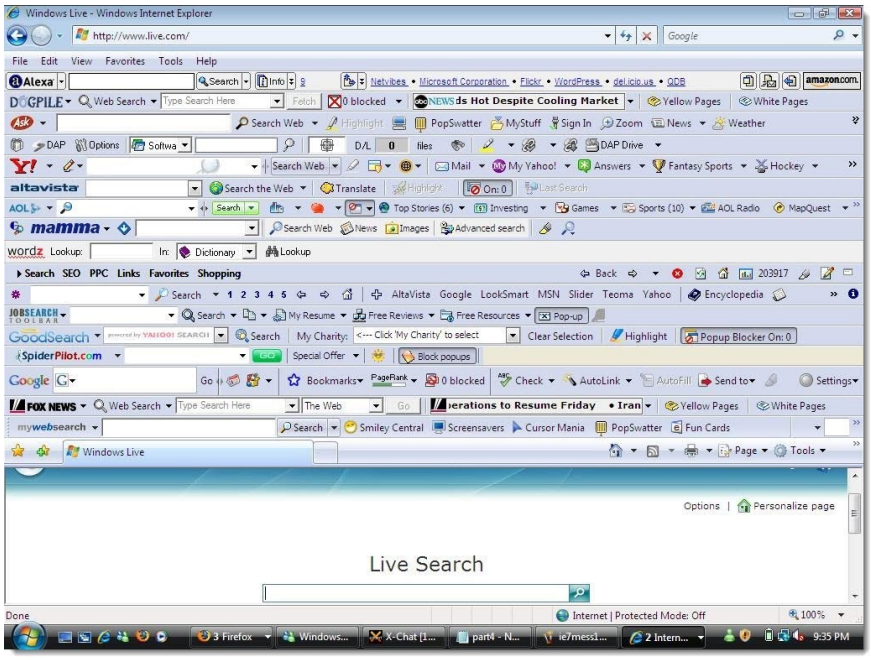
After making sure the malware: adware and spyware have been completely removed from your system, you can then reconnect the Internet on the system.

Before reconnecting to the Internet, reset your browser and the homepage (homepage).

Make sure your HOSTS file has not been hacked.

7. Clean the browser

Even if the above methods work, however, these adware may have infected your browser and uninstalled the program can not remove adware. To clean the browser, you just need to reset its search engine (if it has changed) and search for extensions or add-ons you don't recognize.

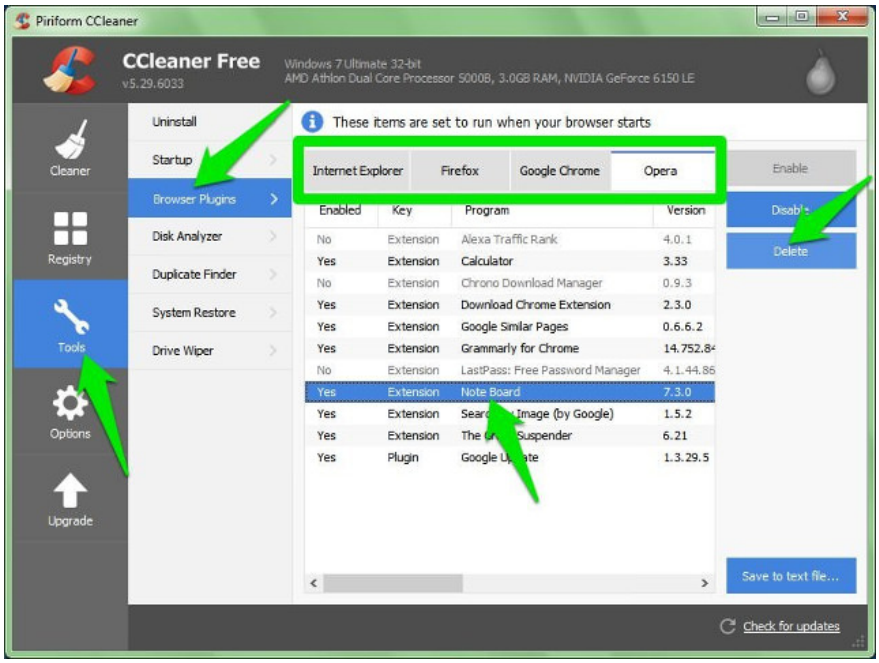


To reset the search engine:

1. Go to the browser settings and find the **Search** title in the **General** section.
2. Select the search engine you want to delete (like Google) from the drop-down menu.

To find extensions or add on adware, you should use a third-party tool to display all extensions and plugins from all browsers in one window, including hidden extensions. There are many third-party tools to help you achieve this like CCleaner's integrated plugin manager.

1. How to use CCleaner software to clean up computer trash effectively



1. Open CCleaner and navigate to the **Tools** section from the left panel.
2. Select Browser Plugins and you will see all the browsers installed in the top bar and the plugins and extensions below them.
3. View each browser and search for the extensions or plugins you've never installed.
4. Select those extensions / plugins and click the **Delete** blue button on the right to delete.

See more:

1. Clean and secure your browser professionally

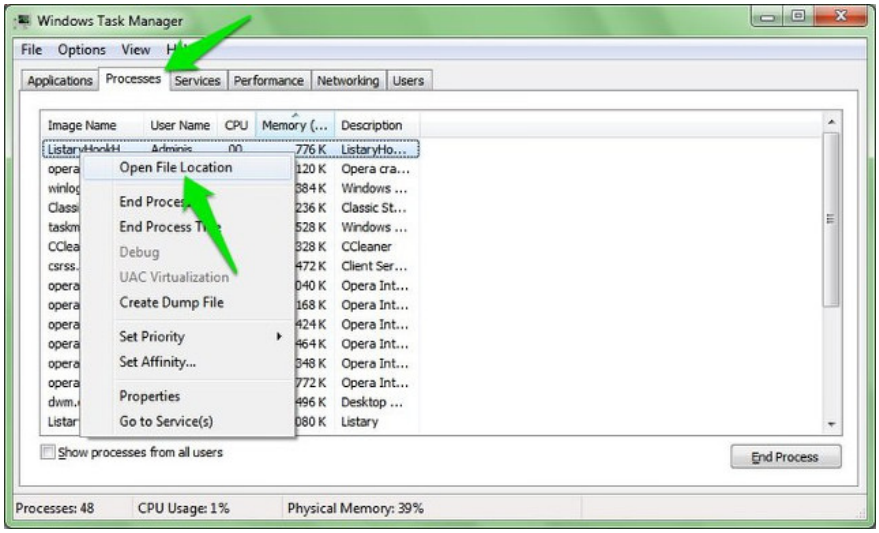
8. Check Task Manager

For normal adware, the above methods are enough, but if you still see the ad, it may be hidden in background services or processes. You can check background processes in Task Manager by pressing **Ctrl + Shift + Esc** and go to the **Processes** tab.

1. All problems about using Task Manager

Next, look for background processes that seem to be hidden, but it's hard to point out the right background process unless you know the name of the adware because Windows lists all its processes here. So you should search the network for the process names you suspect and if it is not a Windows process, follow the steps below:

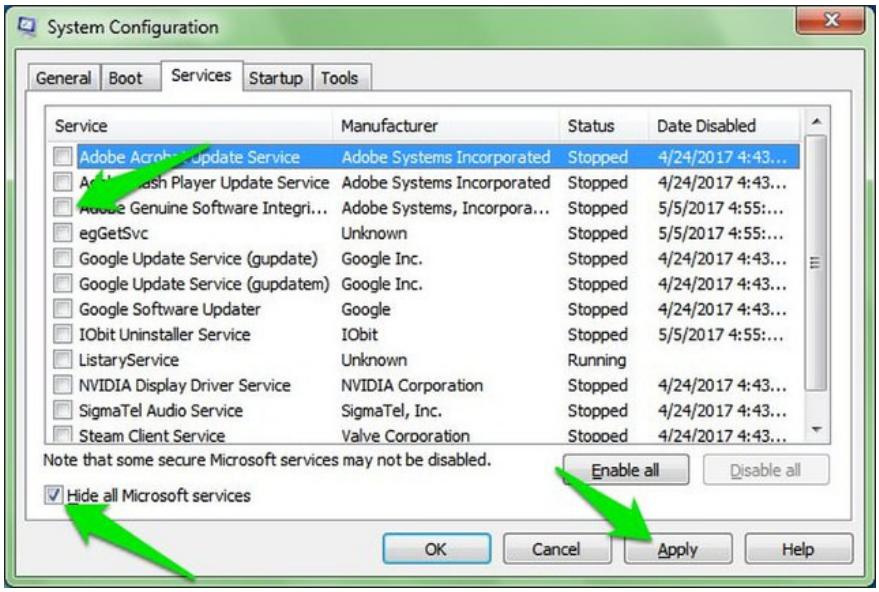
1. Right-click it and select **Open File Location** .
2. Delete all data you see.
3. If you can't delete it, then return to Task Manager to finish the process and then try deleting again.



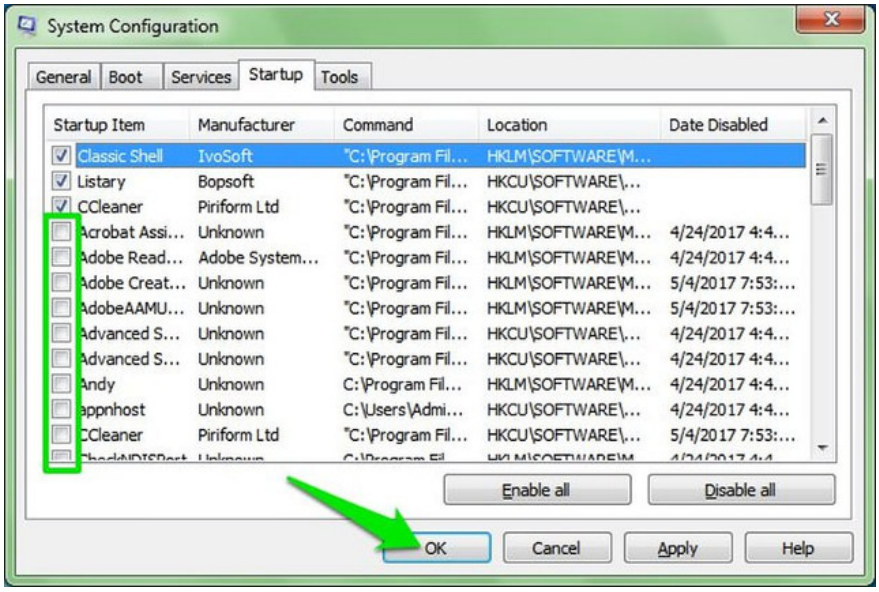
9. Turn off startup programs and services

This method has been used by many people to disable advertising and fake programs and it can fix your problem.

1. Press the **Windows + R** keys and enter **msconfig** in the **Run** dialog box to open the system configuration window.
2. Go to the **Services** tab here and select the checkbox next to **Hide all Microsoft services** .
3. View this list and uncheck all services you don't recognize or need to start with the system.
4. Click the **Apply** button below to confirm the change.



Switch to the **Startup** tab and you'll see all the programs start up. Users of Windows 8 and 10 will have to open **Task Manager** and go to the **Startup items** tab to see the startup programs. Just uncheck the checkbox next to unrecognized startup programs and apply changes.



You will have to restart the computer for these changes to take effect and see if the adware stops. If you find it effective, you should run AdwCleaner to find adware because when you stop the service, it is not hidden from starting up.

1. Turn off programs that start with the system on Windows 10

10. Boot in Safe Mode

If the above methods do not work, you can try booting the computer in Safe Mode. When in Safe Mode, it only downloads the necessary system files and drivers, very rarely fake programs can 'survive' in Safe Mode. Then run AdwCleaner from Safe Mode to remove the adware.

11. Prevent Adware and Spyware

After removing adware, learning how to avoid these software in the future is also a way to 'prevent more than cure'. You can do it the following way:

If you are suspicious of any program or software, search on Google

A very simple but effective rule to keep safe on the Internet is when you suspect an application or file, the best way is to search on Google rather than download and test yourself. The search formula is simply 'program x is malware or advertising?'.

Avoid downloading crack software

If you like to access torrent sites to "steal" copies of legitimate paid applications, you may be infected with adware and malicious software.

Cracking software of paid programs is often infected with malware and advertising, causing serious harm to computers. Therefore, you should only download programs from the main site and do not download crack

programs.

Do not download anything suggested

The Internet is full of advertisements that require you to download a great program to get the best benefits, such as' download this money-making program to become a millionaire 'or' this free auto x bot will do auto x jobs, etc. If you listen to these enticements, there's a chance you'll have to clean up or reset your computer.

1. 4 ways to reset the Windows computer to its original state

Read the steps when installing the program

There are many adware that sneak in the same legitimate program as an attachment. While installing legitimate programs, it will trick you to determine installing it. The simple solution is that while installing any program, check the steps carefully and look for checkboxes that require you to install other programs with the main program.

The installer can also directly request the installation of a specific program and only gives you the option to click on **Next** or **Decline** , you should choose **Decline.**

Also, if the installer has the option of **Custom Installer** or similar, select this option. The program may not suggest this option, but this is a trick to make sure you haven't removed the hidden programs.

It is important to check the installation steps manually, and you should do it every time you install the program. However, there is a faster way of installing the **Unchecky** application to automatically reject or deselect the recommended programs.

Removing malicious, adware as soon as possible is important not only because it annoys you but also makes you download more adware and even malicious software can be harmful. for computer or steal your data.

Although the way above is enough to remove any adware, you should also restore your computer to a previous or reset time to remove any type of adware or malicious software.

1. Instructions on how to use System Restore on Windows

Finally ensure that your Web browser security is absolutely secure.

Refer to some of the following articles:

1. Summary of the most frightening "virus worms" on computer systems

1. 9 most effective antivirus software for Windows today

1. Troll friends by creating "fake" virus on Notepad

Good luck!