

Remove Adware, pop-ups, and browser redirects from your Windows PC

This article helps you recognize, avoid and remove Adware from Windows computers. Free your PC from annoying browser ads, intrusive pop-up adverts, and browser redirects.

What is Adware?

Adware is a form of ad-based software, a form of monetization that allows the developer to offer products for free to the public but still get paid by an advertising company. In exchange for a fee, the developer will either put together code that will display advertisements for the ad network or convince the user to install software from another vendor along with the original product. Adware can be dangerous. The line between adware and spyware is so fine and blurred that the initial offering may include more than you would have liked. Ads, which may be pop-ups or videos, may not be a problem at first, but behind them may be a suspicious program monitoring the user's activity, establishing a shadow pattern of browsing habits, or encouraging them to purchase a product through an affiliate network.



There is certainly controversy about ad-supported software, and that's because some e-book readers, phones, and messaging apps include this type of software and also require user consent for certain benefits. Occasionally, companies include information about adware in terms and conditions or in the end-user license agreement. However, who has the patience to read all the way through? Aggressive adware is not harmless and has so far attacked a significant number of known and trusted applications.

How to avoid Adware

There are very rarely signs that a program would run in the background or that suspicious files have been installed on your computer. Even security software can face some problems when it comes to adware, and that's because there are legitimate services that come bundled with ad-based software. Even if detecting adware is difficult, it is almost impossible to determine the extent of the damage. Often, advertising companies illicitly combine open-source applications with adware, and this sometimes happens against the wishes of the developer. To distribute these unofficial ad-supported software kits, advertisers trick the original website itself and register domains for the purpose of typo-squatting.

If you use a cybersecurity solution, there's not much left to do. A simple scan will reveal all suspicious files and programs which you can then delete with a single click. Security solutions also give users the option to disable adware detection, but this isn't necessarily a good idea if you want complete network protection.

After all, it's up to each user to be careful what they install on their devices. So, make sure you download files that only come from trusted shops, such as the app's official website, and that you pay attention to all installation steps. If you see that the app you want to install comes bundled with a "special offer", make sure you don't install that too by unchecking the box next to it or pressing the Cancel button.

Eliminate Adware on Windows: annoying apps, toolbars & browser add-ons

To get rid of annoying adware, so you can enjoy a pleasant Internet browsing experience, follow the instructions below:

Step 1

Try to uninstall all the unknown programs from your computer:

Go to Start > Control Panel > Programs > Programs and Features and double-click on each of the unknown/unwanted applications to remove them from the system. For more details, read – [How to uninstall or remove apps and programs in Windows](#).

Step 2

Now you should be able to change your browser's homepage, search engine and get rid of any unwanted add-ons/extensions:

If you are using **Mozilla Firefox**, [here are the steps to take](#).

If you are using **Google Chrome**, follow the steps described in the articles below:

- [How to set your homepage in Google Chrome](#)
- [How to set your search engine in Google Chrome](#)
- [How to manage extensions in Google Chrome](#)

If you are using **Microsoft Edge**, use the articles below:

- [How to change the home page in Edge](#)
- [Set your search engine in Edge](#)

If you are using **Internet Explorer**, here are the articles:

- [How to change the home page in Internet Explorer](#)
- [Set your search engine in Internet Explorer](#)
- [Manage the add-ons in Internet Explorer](#)

Step 3

Block notifications from the websites allowed to display messages on your screen by following these steps:

- [Turn off notifications in Google Chrome](#)
- [Turn off notifications in Mozilla Firefox](#)
- [Turn off notifications in Microsoft Edge](#)

Step 4

To be able to block future ads, we recommend you install Adblock Plus for your browser:

- [Adblock Plus for Mozilla Firefox](#)
- [Adblock Plus for Google Chrome](#)
- [Adblock Plus for Microsoft Edge](#)
- [Adblock Plus for Internet Explorer](#)

Step 5

Perform a disk cleanup to reduce the number of unnecessary files on your drives (this can also help your PC run faster). You can follow the instructions [presented here](#).

If after restarting the computer the situation persists, please open a support ticket that includes [a BDSYS log](#).