

Windows laptops & PCs | Medium | 2 min read

Removing adware and unwanted toolbars, and resetting your browser

If your browser has a home page you did not choose, extra toolbars, endless adverts or searches that go to strange sites, you probably have adware or an unwanted extension. This can usually be cleaned up safely.

Step 1: remove unfamiliar programs

1. Windows 11: open **Settings, Apps, Installed apps**. Windows 10: open **Settings, Apps, Apps & features**.
2. Sort by **Install date**. Look at recent items you do not recognise or did not install on purpose.
3. Click the program, then **Uninstall**.

If you are unsure, search the name online first, or ask us. Do not remove things you need, such as drivers, Microsoft items or your antivirus.

Step 2: remove browser extensions

- **Microsoft Edge**: click the three dots, then **Extensions**, then **Manage extensions**. Remove ones you do not recognise.
- **Google Chrome**: click the three dots, then **Extensions**, then **Manage Extensions**, and click **Remove**.

Step 3: stop notifications from websites

In Edge or Chrome, open **Settings**, then **Privacy** (or **Cookies and site permissions**), then **Notifications**, and remove sites you do not know.

Step 4: scan the PC

Run a **Full scan** in **Windows Security**, as in our guide on virus scans.

Step 5: reset the browser

This puts the browser's settings back to normal.

- **Edge**: **Settings, Reset settings, Restore settings to their default values**.
- **Chrome**: **Settings, Reset settings, Restore settings to their original defaults**.

Your bookmarks and saved passwords are normally kept, but extensions are turned off and the start page and search engine go back to default. Check the details on the screen before you confirm.

Download only from the maker's website, untick extra offers during installation, and never click **Allow** on a notification you did not expect.

When to get more help

Get in touch if adverts or pop-ups return after the reset, if you entered a password or card details on a suspicious page, or if a warning page gives a phone number. Do not ring it.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.