Trojan Virus - what it is, classic tricks, and how to avoid and remove it

Gridinsoft Help Center

What it is

A trojan is malware that pretends to be something helpful (an app, document, or script) but does something harmful once you run it. Unlike a worm or classic "virus," a trojan doesn’t spread by itself - it needs you to open or install it. Common trojan families steal passwords, spy on activity, or pull in more malware. Overview and examples: https://gridinsoft.com/trojan

Why it matters

One click can give criminals a foothold on your PC - leading to stolen logins, drained accounts, or even a later ransomware hit.

How it works

- Disguise: arrives as a "must-have" app, crack, driver, invoice, or update.
- Execute: you open it; the trojan runs and installs quietly.
- Payload: steals data, spies, changes settings, or downloads more malware.
- Persist: adds startup entries or tasks so it returns after reboot.

Red flags

- Prompts to disable antivirus or run as admin for a "viewer/codec."
- Files from torrents or random sites that ask for unusual permissions.
- New tray icons, toolbars, or background network traffic you don’t recognize.
- Passwords suddenly stop working or you see logins from new locations.

Do it right

- Get software and updates only from official vendor sites or trusted stores.
- Don’t open unexpected attachments; scan downloads before running.
- Keep Windows, your browser, and security tools updated with real-time protection on.
- If you suspect a trojan: disconnect from the internet, run a full scan, change passwords from a clean device, and remove unknown startups; reimage if problems persist.