Rogueware - fake antivirus scams, red flags, and how to remove them

Gridinsoft Help Center

What it is

Rogueware (aka scareware or rogue security software) is a fake antivirus/optimizer that pretends your PC is infected, then pushes you to pay for a "full version" to fix invented problems. It uses alarming pop-ups, fake scans, and urgent timers to pressure quick clicks. Once installed, it may block real security tools, alter browser settings, and pester you with more purchase prompts.

Why it matters

You can lose money, install more malware, and disable real protection while thinking you’re safer.

How it works - quick tour

- Flashy ads or pop-unders claim instant infection.
- A trial "scanner" always finds dozens of fake threats.
- Paywall pop-ups demand a license to clean them.
- Some variants add adware or steal card details.

Red flags

- Security alerts that look off-brand or full of typos.
- Tools demanding payment before removing "threats."
- Blocked access to Task Manager or your real antivirus.
- Browser homepage/search suddenly replaced.

Prevent it

- Download software only from vendor sites or trusted stores.
- Keep Windows and your AV updated; ignore web pop-up "virus alerts."
- If installed, disconnect, uninstall the rogue, run a reputable scanner, and reset browsers.