Scareware - fake virus alerts, telltale signs, and how to avoid them

Gridinsoft Help Center

What it is

Scareware is fake security or system-cleaning software that tries to panic you into installing it. It throws alarming pop-ups ("Your PC is infected!"), runs bogus "scans" that always find problems, and demands payment or a download to fix them. Once installed, it may steal data, show more ads, or block real security tools.

Why it matters

Scareware drains money, exposes personal data, and can open the door to more malware - all while giving a false sense of safety.

How it works

- Flashy web pop-ups or fake system alerts claim instant infection.
- A "free scan" pretends to find dozens of threats.
- A paywall or download is pushed as the only fix.
- After install, it nags for upgrades, hijacks settings, or adds more unwanted apps.

Red flags

- Alerts full of typos, generic names, or branding that doesn’t match your antivirus.
- Demands to pay before removing "threats."
- Instructions to call a phone number or allow remote control.
- Browser homepage/search suddenly changed after clicking an "urgent" alert.

Prevent it

- Ignore infection pop-ups from websites; use your installed security app to scan instead.
- Download software only from vendor sites or trusted stores.
- Keep Windows and your security tools updated.
- If you installed scareware, disconnect from the internet, uninstall it, run a reputable scan, and reset browsers.