FakeAV (Fake Antivirus): What it is, classic red flags, and how to remove it safely

Gridinsoft Help Center

What it is

FakeAV is scareware that pretends to be antivirus. It fakes "deep scans," invents dozens of threats, and pressures you to pay for a bogus cleanup-or it quietly installs more malware. Learn the telltale signs in our FakeAV explainer.

What you may notice

- Alarming pop-ups: "Critical infection! Click to remove."
- A "scanner" you never installed suddenly runs at startup
- Demands for payment before fixing anything
- Browser/homepage changes or new toolbars

How it gets in

- Malicious ads and fake "Your PC is infected" pages
- Bundled with sketchy "free" utilities or cracks
- Phishing attachments and look-alike download sites

Remove it now (quick steps)

- Disconnect from the internet.
- Uninstall the suspicious app and end its processes.
- Run a full anti-malware scan, reboot, and scan again.
- Restore browser settings; remove unknown extensions.
- From a clean device, change passwords and enable MFA.

Prevent it

- Download software only from official sources; avoid cracks and "free scanners."
- Keep Windows, browsers, and security tools updated.
- Use reputable real-time protection and consider DNS/web filtering.
- Teach everyone to treat scare-popups as red flags-close the tab, don’t click.