

PUABundler - what it is, risks, and how to avoid it

Gridinsoft Help Center

What it is

Why it matters

Bundles erode trust, expand attack surface, and can pave the way for adware, trackers, or later malware.

How it spreads

- Third-party download managers and mirror sites
- Fake "update your codec/driver" prompts
- Aggressive affiliate campaigns and dark-pattern pages

How to spot it - quick checks

- Multiple "offers" or "optional components," often pre-checked
- Express vs Custom path with buried controls
- Unexpected search/homepage changes, new extensions, extra tray apps

What to do

- Get the app from the vendor's official site.
- Uninstall add-ons; remove unknown extensions.
- Review startup entries, scheduled tasks, and services.
- Run an anti-malware scan; reset browsers if hijacked.

Watch-outs

- Some bundles install an auto-updater that brings the junk back after a restart. After cleaning, reboot and check again.
- Even if you click Decline, the installer may still add telemetry, tasks, or small helper apps. Remove anything you don't recognize in Apps & Features, Startup, and Scheduled Tasks.