

FusionCore - What it is, how it sneaks in, and how to remove it safely

Gridinsoft Help Center

What it is

What you may notice

- New apps or browser extensions you didn't choose
- Homepage/search engine changed, extra ads or redirects
- Startup gets slower - background updaters and tasks appear
- Security tools warn about PUPs or unwanted changes

How it gets in

- Bundled installers from download portals and "free" repacks
- Fake update prompts and deceptive setup wizards with pre-checked offers
- "Next, next, finish" installs without custom options

Remove it now - quick steps

- Uninstall unfamiliar programs and browser add-ons.
- Run a full anti-malware scan, reboot, then scan again.
- Reset browser homepage/search and clear cache; remove leftover tasks/services.
- From a clean device, change passwords if you installed anything highly suspicious.

Prevent it

- Download from official sites - avoid mirrors and repacks.
- During install, pick Custom/Advanced and uncheck extras.
- Keep Windows, browsers, and security tools updated.
- Consider DNS/web filtering to block known bad hosts.