

CoinMiner: What it is, signs to spot, and how to remove cryptojacking malware

Gridinsoft Help Center

What it is

CoinMiner is malware that hijacks your computer's CPU/GPU to mine cryptocurrency for someone else. You get slowdowns, heat, and bigger power bills; they get the coins. See common signs and fixes in our [CoinMiner guide](#)

What you may notice

- Fans roaring and laptop getting hot when you're idle
- Apps lagging; games drop frames; battery drains fast
- Task Manager shows high CPU/GPU from unknown processes
- Power bill spikes; browser tabs that pin CPU

How it gets in

- Cracked "free" software and fake updates
- Phishing attachments or droppers from other malware
- Rogue browser extensions or scripts that run mining code in tabs

Remove it now (quick steps)

- Disconnect from the internet.
- Run a full anti-malware scan and reboot.
- In Task Scheduler/Startup, remove unknown items; uninstall shady extensions.
- Update OS, drivers, and browser; clear browser cache and site data.

Prevent it

- Install software only from official sources; avoid cracks.
- Keep OS, browsers, and security tools updated.
- Use real-time protection and consider blocking known mining scripts.
- Watch Task Manager: if idle usage isn't idle, investigate.