Keylogger - What it is, warning signs, and how to remove and prevent it

Gridinsoft Help Center

What it is

A keylogger is spyware that records what you type - passwords, messages, credit card numbers - and often tracks clicks and screenshots too. Criminals bundle it inside shady installers, phishing attachments, or cracks. For background and cleanup tips, see our keylogger explainer.

What you may notice

- Sudden re-prompts for logins or missing 2FA texts
- New startup items, browser extensions, or a "helper" you did not install
- Odd spikes in network traffic when you are idle
- Brief command windows that open and close quickly

How it gets in

- Phishing emails and macro-enabled documents
- "Free" repacks, keygens, and fake updates
- Drive-by downloads from risky sites

Remove it now

- Disconnect from the internet to stop data exfiltration.
- Run a full anti-malware scan, reboot, then scan again.
- From a clean device, change passwords and turn on MFA for email, banking, and cloud.
- Check startup items, scheduled tasks, services, and extensions - remove unknowns.
- Watch accounts for unusual logins and sign out of other sessions.

Prevent it

- Install software only from official sources - avoid cracks and repacks.
- Keep OS, browsers, and Office updated and block macros by default.
- Use EDR or reputable anti-malware with real-time protection.
- Enable MFA everywhere so stolen passwords are less useful.
- Consider DNS and web filtering to block malicious sites.