Carberp Banking Trojan: Signs to spot and steps to stay safe

Gridinsoft Help Center

Carberp is a sneaky banking trojan-malware that slips onto your PC, watches what you type, and tries to steal money-related data. It targets things like online banking logins, card details, and one-time codes, often without any obvious signs.

How it gets in:

- Fake emails and download links (phishing)
- Cracked software and malicious installers
- Outdated browsers, plugins, or document macros

What you might notice:

- Unexpected pop-ups on banking pages asking for extra info
- Browser feels slow or crashes during logins
- New extensions or startup items you didn’t add

If you suspect it, do this now:

- Disconnect from the internet; avoid logging into banks.
- Run a full scan with trusted anti-malware and remove findings.
- From a clean device, change banking/email passwords and enable MFA.
- Contact your bank to review recent activity and add alerts.

How to prevent it:

- Keep Windows, browser, and security tools updated.
- Don’t open unknown attachments or run untrusted installers.
- Use strong, unique passwords (manager helps) + MFA.
- Limit browser extensions; only install from trusted sources.