Banker Trojan: What it is, how it steals logins and money, and how to remove it

Gridinsoft Help Center

What it is

A banker trojan is malware built to steal money from online banking. It sneaks onto a PC, watches logins, and can secretly redirect you to fake pages or overlay real ones to grab passwords, 2FA codes, and payment details. It often hides by adding startup tasks and registry entries so it comes back after reboot.

What you may notice

- Banking pages look slightly different or ask for extra info
- Random redirects during checkout or login
- New browser extensions or changed homepage/search
- Unusual logins, transfers, or MFA prompts you did not trigger

How it gets in

- Phishing emails and booby-trapped attachments
- Fake updates or cracked software installers
- Malvertising and drive-by downloads on risky sites

Remove it now (quick steps)

- Disconnect from the internet; avoid opening banking sites.
- Run a full scan with trusted anti-malware and reboot.
- From a clean device, change bank/email passwords and enable MFA.
- Call your bank, review recent transactions, and set alerts.
- Check startup items, scheduled tasks, services, and extensions; remove unknowns.

Prevent it

- Install software only from official sources; skip cracks.
- Keep Windows, browsers, and extensions updated.
- Block macros by default; be cautious with attachments.
- Use a password manager and unique passwords + MFA.
- Bookmark bank sites and navigate from bookmarks, not links.