# FormBook - What it is, how it steals data, and how to remove it safely

Gridinsoft Help Center

## What it is

FormBook is spyware for Windows that sneaks onto a PC to steal files and data. It can log what you type, grab passwords and cookies from browsers, and take screenshots, then send everything back to the attacker. Details and IOCs: see our FormBook explainer.

## What you may notice

- Sudden logouts or new MFA prompts you didn’t start
- Unknown browser extensions or odd redirects
- Network spikes after opening an email or installer
- Apps crash or settings change without reason

## How it gets in

- Phishing emails with booby-trapped attachments
- Fake updates and bundled "free" installers
- Malvertising and shady download sites

## Remove it now - quick steps

- Disconnect from the internet and avoid banking or email on the infected device.
- Run a full anti-malware scan, quarantine findings, reboot, then scan again.
- From a clean device, change passwords and enable MFA.
- Review startup items, scheduled tasks, and extensions - remove unknowns.
- Move any crypto to new wallets with fresh seed phrases.

## Prevent it

- Install software only from official sources - avoid cracks and repacks.
- Keep Windows, browsers, and plugins updated.
- Use reputable EDR/anti-malware plus email/web filtering.
- Be cautious with attachments - block macros by default and preview links before clicking.