Crimeware: What it is, common examples, and how to protect yourself

Gridinsoft Help Center

Why it matters

Crimeware aims for cash and data. That means drained accounts, stolen identities, locked files (ransom), hijacked social profiles, and business downtime.

How it shows up

- Phishing & fake pages that grab logins
- Malicious installers/updates and cracked software
- Drive-by ads and rogue extensions
- Weak remote access (RDP/VPN) and unpatched apps

Signs to watch

- Sudden MFA prompts, unknown logins, or new rules in email
- Ransom notes, missing files, or changed extensions
- High CPU/GPU, fans roaring when idle; odd network spikes
- Security tools disabled or updates failing

If you suspect crimeware (first steps)

- Disconnect from the network.
- Scan and quarantine with trusted anti-malware; reboot and scan again.
- From a clean device, change passwords and enable MFA.
- Check accounts, bank/cards, and email forwarding rules; alert your bank/IT.

Prevent it

- Install software/extensions only from official sources.
- Keep OS, browsers, and apps updated; patch internet-facing services fast.
- Use a password manager + unique passwords + MFA.
- Train your team/family to spot phishing; consider DNS filtering/EDR.
- Keep offline, tested backups in case of ransomware.