Djvu (STOP) Ransomware: What it is, how it spreads, and how to recover safely

Gridinsoft Help Center

What it is

How it spreads

- Bundled with cracked "free" software and fake installers
- Malvertising and deceptive download sites
- Phishing attachments (archives, scripts) and shady browser extensions

What you may notice

- Documents/photos won’t open; filenames show a new extension
- Ransom note files across folders
- CPU/disk spikes; security tools crash or get disabled

If it hits

- Isolate the PC (turn off Wi-Fi/unplug; disconnect external/network drives).
- Keep ransom notes and logs-useful for recovery and investigation.
- Check offline backups; rebuild on a clean image and restore data.
- From a clean device, change passwords and enable MFA.
- Identify the entry point (installer, phish, extension) and block it.

Prevent it

- Avoid cracks and unofficial download sites; install from trusted sources only.
- Keep Windows, browsers, and plugins updated.
- Use reputable EDR/anti-malware and email/web filtering.
- Maintain offline, tested backups and practice a restore.
- Train users to spot phishing and fake update prompts.