CryptoLocker Ransomware: What it is, warning signs, and how to recover safely

Gridinsoft Help Center

What it is

CryptoLocker is ransomware that breaks into a Windows PC, hunts for documents (on the computer and connected drives), encrypts them with strong keys, and then demands a payment to unlock your files. You'll see a ransom note saying your data is locked and a deadline is ticking.

What you may notice

- Files won't open and may have new extensions
- A ransom message on the desktop or in many folders
- Backups on attached or network drives also unusable
- Security tools disabled; sudden spikes in CPU/disk activity

If it hits (act fast)

- Isolate the PC (unplug network/Wi-Fi; disconnect external drives).
- Don't delete ransom notes or logs-they can help recovery.
- Check for offline backups; rebuild the system clean and restore data.
- From a clean device, change passwords (email/admin) and enable MFA.
- Ask IT/IR to identify the entry point and block related domains/IPs.

Prevent it

- Keep Windows and apps patched; remove or lock down remote access (RDP/VPN).
- Use reputable EDR/anti-malware and email filtering.
- Maintain offline, tested backups (and practice restores).
- Train users to spot phishing and fake updates.
- Use least privilege and MFA for all important accounts.