Cyberterrorism: What it is, how it strikes online, and how to prepare and respond

Gridinsoft Help Center

Cyberterrorism

What it is

Cyberterrorism is using computers and the internet to frighten, disrupt, or harm people and organizations-at scale. Instead of bombs or break-ins, attackers use hacks, fake messages, and takedowns to shut services, spread fear, or pressure governments and companies.

What it looks like

- Website and service takedowns (DDoS): flooding a site so citizens can’t get news or services.

- Hacks and data leaks: stealing sensitive files, then publishing them to intimidate.

- Ransomware & malware: locking systems to halt hospitals, transport, or utilities.

- Disinformation & phishing: crafted messages to mislead, panic, or gain access.

Why it’s different

The goal isn’t just money - it’s impact and fear: interrupt emergency lines, jam public portals, or erode trust in official info.

How to reduce the risk

- Harden the basics: MFA everywhere, patch fast, least-privilege access.

- Protect the edge: WAF/DDoS shielding, rate limits, and geo/IP rules.

- Plan and practice: incident runbooks, backups you’ve actually restored, and clear comms templates.

- Train people: spot phishing, verify urgent requests out of band, report quickly.

If you’re targeted

- Stabilize services (activate DDoS protection, switch to read-only modes if needed).

- Contain and investigate (isolate infected hosts, preserve logs, rotate credentials).

- Communicate clearly to users and partners; don’t speculate.

- Restore from clean backups and review gaps before re-opening everything.