Brute Force Attack: What it is, signs to watch for, and how to stop it

Gridinsoft Help Center

What it is

A brute force attack is password guessing on turbo. An attacker tries lots of combinations - sometimes millions - until one works. It’s not clever, just relentless, and it targets anything with a login or key: email, Wi-Fi, cloud apps, even encrypted files.

How it works (quick tour)

- Online guessing: rapid logins against your account (or slower to dodge lockouts).

- Password spray: the same common password tried across many users.

- Offline cracking: stolen password hashes or encrypted files are attacked with powerful hardware and wordlists.

What you might notice

- Repeated login alerts or MFA prompts you didn’t start

- Account lockouts at odd hours

- Security emails about new sign-in attempts or locations

Quick defenses

- MFA everywhere: app codes or security keys beat guesses.

- Strong, unique passwords: use a manager; avoid repeats.

- Lockouts & rate limits: after a few bad tries, pause or block.

- Blocklists & allowlists: deny risky countries/IPs; require VPN for admins.

If you’re being targeted

- Change the password to a unique, long one (from a clean device).

- Turn on MFA and remove weak fallback methods (SMS only, security questions).

- Review sessions/devices; sign out everywhere and revoke unknown tokens.

- Check recovery options (email/phone) and reset them if needed.

- Notify your provider/admin to enable extra throttling or IP blocks.