MFA (Multi-Factor Authentication) - What it is and the safest ways to use it

Gridinsoft Help Center

What it is

Multi-Factor Authentication (MFA) adds an extra check when you sign in, so it is not just a password. You confirm with something you know (password) plus something you have or are. For a short primer, see our MFA explainer.

Why it matters

If a password leaks, MFA is the speed bump that stops account takeovers. It is one of the highest impact, lowest effort protections you can turn on today.

How it works - quick tour

- Password + one more factor to prove it is really you
- Something you have: phone code, authenticator app, hardware key
- Something you are: fingerprint or face on a trusted device
- Step-up prompts for risky logins, new devices, or unusual locations

Good choices in order

- Hardware security key (phishing resistant)
- Passkeys or platform biometrics
- Authenticator app codes or push approvals
- SMS codes only if nothing else is available

Quick setup tips

- Turn on MFA for email, banking, cloud storage, socials first
- Prefer keys, passkeys, or app codes over SMS
- Generate backup codes and store them safely offline
- Add two sign-in methods so you are not locked out if a phone is lost
- For teams: require MFA with SSO and review exceptions regularly