Multi-Factor Authentication FAQ

Answers to the questions every team has about MFA

What Is Multi-Factor Authentication?

Multi-factor authentication (MFA) requires two or more pieces of evidence before granting access to an account. Typically that means something you know (a password), something you have (a phone or hardware key), and/or something you are (a fingerprint or face scan). Even if a criminal steals your password, they still cannot log in without that second factor.

Does My Business Really Need It?

Yes. Microsoft reports that MFA blocks more than 99.2% of automated account compromise attempts. Most cyber-insurance policies, vendor contracts, and compliance frameworks now require MFA on email, remote access, and admin accounts. If you only do one thing for security this year, turn on MFA.

What Are the Different MFA Methods?

- Authenticator apps (Microsoft Authenticator, Duo, Google Authenticator) — recommended
- Hardware security keys (YubiKey, Feitian) — strongest option, phishing-resistant
- Push notifications — convenient but vulnerable to MFA-fatigue attacks
- SMS or email codes — better than nothing, but vulnerable to SIM-swapping
- Biometrics — great for unlocking devices, often paired with another factor

Common Concerns

- 'It will slow my team down' — most logins prompt only every 30–90 days per device
- 'What if I lose my phone?' — backup codes and admin recovery handle this safely
- 'It's expensive' — most business email and cloud platforms include MFA at no extra cost
- 'My users will revolt' — clear communication and a 1-week ramp eliminate friction

Where Should You Enable MFA First?

Start with the highest-risk accounts: email, remote access (VPN, RDP), administrator and finance accounts, password managers, and any system holding customer or health data. Then expand to every cloud application your team uses. Directive Technology can roll out MFA across your environment with a clear plan that minimizes disruption.