DefineEdge

What Is MFA - and Why Your Insurance Requires It

A plain-English guide to multi-factor authentication and cyber insurance requirements

What MFA Actually Is

Multi-factor authentication (MFA) means proving who you are with more than just a password. It combines something you know (your password) with something you have (your phone, an authenticator app, or a hardware key). Even if a password gets stolen or guessed, an attacker still can't get in without that second piece.

Why Passwords Alone Aren't Enough Anymore

- **Reused passwords** - the same password used across multiple sites means one breach elsewhere can unlock your accounts.
- **Convincing phishing pages** - fake login pages are good enough now that even careful people get fooled.
- **Automated guessing tools** - attackers use software that tries thousands of password combinations in minutes.

A password-only login is a single lock on the front door. MFA adds a second, independent lock that the same stolen key can't open.

Why Cyber Insurance Requires It

Carriers have paid out enough breach claims to know that the overwhelming majority trace back to one compromised login with no second layer of protection. That's why MFA now shows up as a hard requirement - not just for email, but for remote access and any account with administrative rights.

Answering "yes" to an MFA question on an insurance application when it isn't fully enforced everywhere can mean a denied claim after a breach. It's worth confirming MFA is actually turned on and required - not just available - before that box gets checked.

Why This Matters

Turning MFA on everywhere it counts is one of the highest-impact, lowest-effort security steps a business can take. It stops the majority of account takeovers cold, and it's increasingly the difference between a covered claim and a denied one.

How to Use This

Share this with whoever is filling out a cyber insurance application or renewal, or with any employee who needs a plain-English reason MFA isn't optional anymore. Keep a copy on file alongside your security documentation.