LESSON 02 OF 05 · 8 MIN · ESSENTIAL

Passwords, MFA and passkeys

Why password reuse is the real problem, what MFA actually protects, and how to roll it out without locking everyone out.

Passwords are a losing game

Complexity rules produce `Summer2024!` and a sticky note. Length and uniqueness matter more. But nobody can remember fifty long, unique passwords, which is why reuse is normal, and why one breach at a random website can unlock your email.

The practical fix is a password manager: it generates long random passwords, fills them in, and stores them in an encrypted vault. You remember one strong master password (or use a passkey), and the tool does the rest.

What MFA really stops

MFA means a password alone isn't enough. Even if someone has your password (from a breach, a phishing page or a reused login), they still need the second factor.

Not all factors are equal:

- **Passkeys** are tied to the real website, so they resist phishing.
- **Authenticator apps** generate a code; good, but a determined attacker can relay it.
- **SMS** is better than nothing, but vulnerable to SIM swap.
- **Push prompts** need number matching, or attackers spam them until someone taps approve.

Rollout without pain

Turn on MFA for the whole platform rather than asking people individually. Make sure two people can administer the service. Print recovery codes and keep them offline. Register a backup device. Then check the sign-in logs for anyone still using a password alone.

Tell staff the one rule that defeats most MFA attacks: **never approve a prompt or share a code you didn't initiate**. If it happens, deny it, change the password and report it.

> NEVER
>
> No bank, IT provider or software company will ask you to read out a code or approve a login. If someone does, it's an attack, even if they know your name, your manager's name and your date of birth.

Key takeaways

- ✓ Reuse is the real password problem; a manager solves it practically.
- ✓ MFA protects you even when a password has already leaked.
- ✓ Passkeys are the strongest common option; SMS is the weakest.
- ✓ Never share a code or approve a login you didn't start.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.