Password Best Practices & MFA Setup

Weak or reused passwords are the easiest entry point for attackers. With credential stuffing attacks using billions of breached passwords, strong unique passwords and multi-factor authentication (MFA) are your essential first line of defense.

Key Points

- ✓ Use unique passwords for every account — never reuse across services
- ✓ Minimum 16 characters with a mix of upper, lower, numbers, and symbols
- ✓ Use a passphrase approach: "correct-horse-battery-staple" is stronger than "P@ssw0rd!"
- ✓ Enable MFA everywhere possible — preferably authenticator apps over SMS
- ✓ Use a password manager (Bitwarden, 1Password, KeePass) to generate and store credentials
- ✓ Never share passwords via email, chat, or sticky notes
- ✓ Change passwords immediately if a breach is suspected
- ✓ Check haveibeenpwned.com regularly for compromised accounts

Action Items

1. Install a password manager and migrate your top 10 most-used accounts this week
2. Enable MFA on all email, banking, and work accounts immediately
3. Replace any passwords shorter than 12 characters with 16+ character passphrases
4. Remove any passwords stored in browsers, notes apps, or spreadsheets

Quick Reference

Strong Password Formula: 16+ chars = 3-4 random words + numbers + symbols (e.g., "Rocket-Mango-42-Sunset!")
MFA Priority Order: Hardware key (YubiKey) > Authenticator app > SMS > Email
Banned: Dictionary words alone, personal info (birthdays, names), keyboard patterns (qwerty, 123456)