Strong Passwords & Multi-Factor Authentication (MFA) Checklist

Create Strong, Unique Passwords

✅ Use **12–16+ characters** — think passphrases ("5PurpleCowsDance@Dawn!") instead of single words.

✅ Mix **uppercase, lowercase, numbers, and symbols**.

✅ Avoid personal info (no birthdays, pet names, or street addresses).

✅ Use a **different password for every account** — especially banking, email, and shopping.

Make Password Management Easy

✅ Use a **password manager** (LastPass, 1Password, Bitwarden) to securely store & auto-fill logins.

✅ Let your manager generate random, complex passwords you don't need to memorize.

✅ Update weak or reused passwords — start with your most sensitive accounts (banking, email, healthcare).

Turn On Multi-Factor Authentication (MFA)

✅ Enable MFA on **all financial accounts**, email, and social media.

✅ Choose **authenticator apps** (Google Authenticator or Microsoft Authenticator) over text message codes when possible — they're harder for criminals to intercept.

✅ If SMS is your only option, it's still better than no MFA at all.

✅ Print or save **backup codes** somewhere secure in case you lose your device.

Keep Devices & Accounts Secure

✅ Turn on **screen locks** and require a PIN, fingerprint, or face recognition.

✅ Don't let browsers save banking passwords.

✅ Watch out for **phishing emails or texts** asking you to "verify" login codes, that's a scam.

Cybersecurity Awareness Month
October 2025