Passwords, Passkeys and Two-Step Sign-In

Most account break-ins start with a stolen or guessed password. These steps stop most of them.

Stronger sign-ins

- **Use passkeys** where offered. You sign in with your fingerprint, face or phone PIN, and there's no password to steal.
- Otherwise, use a **long passphrase** of 4 or more random words, different for every important account.
- Let a **password manager** (built into your phone or browser) remember them for you.
- Turn on **two-step sign-in** for email, banking and social media.

Protect your phone number

- Ask your carrier to add a **PIN or "port-out" lock** to stop SIM-swap attacks.
- **Never share a code** sent to your phone. No real company will ask for it.
- If you suddenly lose phone service, call your carrier right away from another phone.

Report it: ReportFraud.ftc.gov | FBI: ic3.gov | Identity theft: IdentityTheft.gov | Age 60+: National Elder Fraud Hotline **833-FRAUD-11 (833-372-8311)**. Free help from Netivo: **(913) 349-3363**.