MISSION VALLEY BANK

MVB 2025 BLOG #3: Cybersecurity Month

Passwords, MFA, and Device Security

One Small Change That Blocks 99% of Hacks

Here's a story: in 2024, a global tech company avoided a multimillion-dollar breach because one employee had multi-factor authentication (MFA) enabled. The hacker had their password, but the extra verification code stopped the attack in its tracks.

This is why passwords, MFA, and device security matter — not just for big companies, but for everyday banking customers and small businesses.

Passwords: The Weak Link

- 123456 and password remain among the most common passwords globally.
- Credential reuse leads to "credential stuffing" attacks across multiple accounts.

MFA: The Game-Changer

- Microsoft reports MFA prevents 99% of account compromise attempts.
- It takes just a minute to set up but adds an enormous security layer.

Device Security: The Overlooked Risk

- Outdated software is a hacker's back door.
- Mobile devices are prime targets for malware, especially with business apps.

Quick Tips:

- Use a password manager — never reuse passwords.
- Turn on MFA for all sensitive accounts (banking, payroll, email).
- Keep all devices updated and enable auto-updates.
- Use biometrics (fingerprint, Face ID) where possible.