MISSION VALLEY BANK

MVB 2025 BLOG #2: Cybersecurity Month

Spotting Phishing & Social Engineering

Would You Click This? The Psychology of Scams

One of the first recorded "phishing" scams dates to the mid-1990s, when hackers tricked AOL users into giving up their login credentials. Thirty years later, the methods are more sophisticated, but the goal hasn't changed: to make you click before you think.

Here's how phishing and social engineering work in 2025 — and how to outsmart them.

Why It Works:

Scams succeed because they target *people*, not systems. Criminals use urgency ("Act now or lose access"), authority ("This is your bank manager"), and curiosity ("Check your prize") to bypass our judgment.

Modern Tricks:

- AI Emails: Scammers use ChatGPT-style tools to write flawless, convincing messages.
- Smishing: Fraudulent texts that look like delivery updates or bank alerts.
- Vishing: Voice phishing — sometimes using AI deepfakes to mimic familiar voices.

Red Flags Checklist:

- Generic greetings (*Dear Customer* instead of your name)
- Urgent deadlines or threats
- Links that don't match the sender's domain
- Unusual requests for sensitive info

Real Example:

In 2023, a UK company lost $240,000 after an employee received a call from what they thought was their CEO. It was a deepfake voice convincing them to wire funds.

How to Protect Yourself:

- Slow down — urgency is a scammer's friend.
- Hover over links before clicking.
- Confirm requests through a second channel (e.g., call your bank directly).
- Share this knowledge with family and employees — awareness is your best defense.

Phishing thrives in silence. Talk about it, share examples, and build a culture of questioning what doesn't feel right.