Keep Your Accounts & Cards Safe From

Social Engineering

What Is Social Engineering?

Social engineering is when a criminal tricks you into giving away private information—like passwords, card numbers, or verification codes—by pretending to be someone you trust.

Common Scams Targeting Your Financial Information

PHISHING EMAILS

Fake emails pretending to be your financial institution.

Look out for:

- "Your account is locked—click to verify."
- Fake statements or alerts.

FAKE "FRAUD DEPARTMENT"

They claim you must "move money to a safe account"—No financial institution will ever ask you to do this.

SMISHING TEXTS

Texts saying your card is locked or that a purchase needs verification.

VISHING PHONE CALLS

Scammers spoof your financial institution's caller ID and pressure you to share:

- **PINs**
- **Passwords**
- **One-time passcodes**

ATM/CARD SKIMMING

Devices on ATMs that steal card data or people watching you type your PIN.

How To Protect Your Accounts & Cards

Never Share:

- PIN
- Passwords
- One-time passcodes
- Full card number

Enable Alerts

- Transaction alerts
- Login alerts
- Online purchase alerts

Verify Before Responding

Don't click links or call numbers sent in a message. Use the number on the back of your card.

At ATMs

- Tug the card reader
- Cover your PIN
- Use well-lit, indoor machines when possible

Use Strong Security

- Multi-factor authentication
- Updated phone & apps
- Avoid public Wi-Fi for banking

If you suspect a scam, change your passwords, review transactions and call us immediately.