CSB

an Altitude Bank™

# PROTECT YOURSELF FROM SCAMS, FRAUD & PHISHING

## COMMON RED FLAGS

Be cautious if a message or call:

- Creates urgency or fear ("Act now!" "Your account will be closed!")
- Asks for personal or financial information
- Requests payment via gift cards, wire transfer, or cryptocurrency
- Comes from an unknown or slightly altered sender (misspelled email or URL)
- Includes unexpected links or attachments
- Promises something that sounds too good to be true

Be suspicious of requests for:

- Gift cards
- Cryptocurrency
- Wire transfers
- Monitor bank and credit card statements regularly
- Set up account alerts for unusual activity
- Freeze your credit if you believe your information was compromised

## BEST PRACTICES TO STAY SAFE

Scammers use email, text messages, phone calls, and social media to trick people into giving away money or personal information. Use these best practices to protect yourself.

- Do not click links or open attachments from unexpected messages
- Hover over links to check the real destination before clicking
- When in doubt, go directly to the official website instead of using the link
- Never share passwords, PINs, or verification codes
- Caller ID can be spoofed — don't trust it alone
- Enable multi-factor authentication (MFA) whenever possible
- Never reuse passwords across banking, email, and work accounts

# PROTECT YOURSELF FROM SCAMS, FRAUD & PHISHING

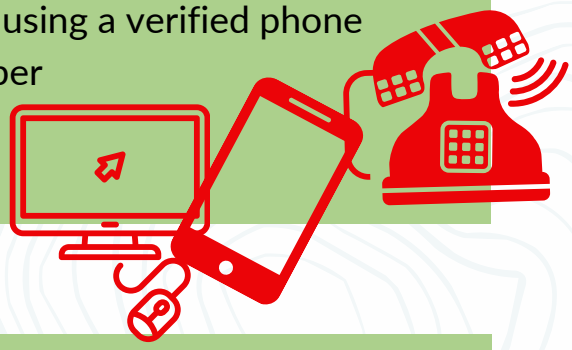
an Altitude Bank™

## E-MAIL & TEXT SAFETY:

- Do not click links or open attachments from unexpected messages
- Hover over links to check the real destination before clicking
- Watch for poor grammar, misspellings, or unusual formatting
- Verify the sender's email address carefully
- When in doubt, go directly to the official website instead of using the link

## PHONE CALL SAFETY:

- Never share passwords, PINs, or verification codes
- Hang up on unsolicited calls asking for payment or information
- Caller ID can be spoofed — don't trust it alone
- Legitimate companies will not pressure you to act immediately
- If unsure, call the organization back using a verified phone number



## WHAT TO DO IF YOU'RE UNSURE:

- Stop — don't respond or click anything
- Verify using a trusted source or official website
- Ask a trusted colleague, family member, or IT/security team
- Report suspicious messages or calls

**WHEN IN DOUBT — DON'T CLICK, DON'T SHARE, DON'T PAY.**

## IF YOU THINK YOU'VE BEEN SCAMMED:

- Immediately contact your bank or credit card provider
- Change affected passwords right away
- Report the incident to:
- Your organization's IT/security team
- Local consumer protection agencies
- The FTC at reportfraud.ftc.gov (U.S.)