CITIZENS
STATE BANK
www.bankcsb.bank

Scam Safety Checklist

Stop • Verify • Protect

Before you act, pause and check

- ☐ Was the contact **unexpected**?
- ☐ Is there **pressure to act immediately**?
- ☐ Are you being told to **keep it secret**?
- ☐ Is payment requested via **gift cards, wire transfer, crypto, or cash**?
- ☐ Are they asking for **passwords, codes, or remote computer access**?
- ☐ Does the story create **fear, urgency, or emotional distress**?

If you checked ANY of these — STOP.

How to verify safely

- ☐ Hang up or close the message
- ☐ Contact the company or person using a **trusted phone number**
- ☐ Ask a family member or trusted friend before taking action
- ☐ Search online for the message or phone number with the word “scam”
- ☐ Take time — **legitimate requests do not expire immediately**

Never do these things

- ☐ Send money to someone you don’t know
- ☐ Pay with gift cards, cryptocurrency, or wire transfers
- ☐ Share one-time passcodes or verification codes
- ☐ Allow remote access to your computer
- ☐ Click links or scan QR codes from unexpected messages
- ☐ Trust caller ID or email names alone

If you think you’ve been scammed

- ☐ Stop communicating with the scammer
- ☐ Contact your **bank or credit card company immediately**
- ☐ Change passwords on affected accounts

☐ Enable multi-factor authentication

☐ Save messages, receipts, and screenshots

☐ Report the scam at **reportfraud.ftc.gov**

☐ Tell a trusted family member or caregiver

Everyday protection tips

☐ Let unknown calls go to voicemail

☐ Keep personal information private

☐ Use spam filters and call-blocking tools

☐ Review bank and credit statements regularly

☐ Have a “trusted contact” for financial decisions

Real organizations do not rush you, threaten you, or demand secrecy.
When in doubt, slow down and ask for help.