CSB

an Altitude Bank™

FRAUD PREVENTION

PROTECT YOURSELF FROM SCAMS, FRAUD & PHISHING

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

Be suspicious of requests for:

- Gift cards
- Cryptocurrency
- Wire transfers
- Promises that sound too good to be true

Scammers use email, text messages, phone calls, and other means to trick people into giving away money or personal information. They use tactics to create fear and panic to then coherse you into providing information.

- These requests can appear to look from a trusted source or business, but instead intend to trick you into clicking and/or providing information.
- Caller ID can be spoofed — don't trust it alone. Hang up, call the known customer service number to validate the conversation or request.
- Legitimate companies will not pressure you to act immediately.

NEVER provide personal information like your SSN or passwords and NEVER provide financial information like bank account #s

SAFEGUARD ALL YOUR ACCOUNTS

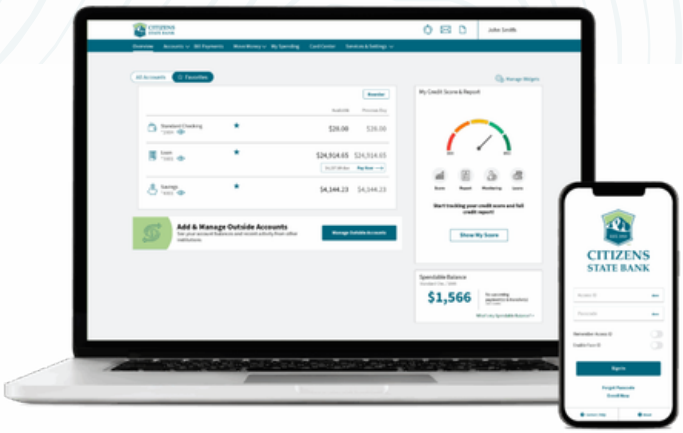
Monitor transactions, Use strong/unique passwords + M.F.A.

REGULARLY REVIEWING YOUR ACCOUNTS IS ONE OF THE EASIEST WAYS TO DETECT SOMETHING UNUSUAL EARLY.

Your Money Matters

STRENGTHEN YOUR CSB ACCOUNTS

A few simple tools in CSB Online Banking and the CSB Mobile App can make a big difference in safeguarding your money.



Turn on Account *Alerts*

Receive real-time notifications for transactions and sign-ins — one of the fastest ways to spot unusual activity.

Use *My Spending*

Categorize your purchases, monitor where money is going, and set spending limits - you'll get alerted when limits are near or exceeded.

Enable *My Credit*

Monitor your credit health, receive credit-related alerts, and keep tabs on any unexpected changes.

Scan to login to your account

EMAIL, TEXT & PHONE SAFETY

- Hover over links to check the real source before clicking (email address and urls/domain names can be 'spoofed' and appear as if they are from a reputable source when in fact they are not. Viewing the source details will show the real sender.
- Watch/Listen for poor grammar, misspellings, unusual sentence structure, or blurry images and logos.
- Login directly to your online account or Application to confirm status. Don't share this login or account details!

IF YOU'RE UNSURE

- **STOP** — don't respond or click anything.
- **VERIFY** — pause and take time to validate the request using a trusted source.
- **ASK FOR HELP** — a trusted colleague, family member, or IT professional can help review.

IF YOU THINK YOU'VE BEEN SCAMMED

1. Immediately contact your bank or credit card provider and change affected passwords and accounts right away.
2. Report the incident to:
   - Local Police
   - Local consumer protection agencies (stopfraudcolorado.gov)
   - The FTC at reportfraud.ftc.gov (U.S.)

CITIZENS STATE BANK
EST. 1913
an Altitude Bank

We are here to help!!

CSBCOLORADO.COM

Member FDIC