Citizens State Bank

Steps to help protect against account takeover fraud...

Account takeover fraud occurs when a fraudster obtains confidential information — including user IDs, passwords, PINs, and token codes — and uses it to access online banking accounts, transfer funds or commit other fraudulent acts. Fraudsters gain access by tricking you to divulge your online banking credentials or installing malicious software (malware) on your devices.

Use this checklist to help reduce your risk of account takeover fraud.

Most users see token prompts only when accessing high-risk payment services (such as Wires, ACH, Foreign Exchange) or administrative functions. Protect your credentials

Protect your tokens! CSB will never ask you for your token PIN or PIN + token code combination in phone calls, emails or text messages.

Implement dual custody. Require all payments or user modifications initiated by one user be approved by a second user on a different device.

Require multi-factor authentication. Add a layer of protection by using multi-factor authentication (MFA) for accessing your company networks, including email, and for payment initiation.

Never click on links from unknown senders. Links and attachments in emails and text messages are a common way to deliver malware. Never click on links or download attachments or install programs without verifying the sender.

Monitor accounts. Reconcile your accounts daily to detect suspicious activity.

Sign up for alert services. Receive a text or email notifications informing you of electronic debits from your accounts.

Update anti-virus software. Reduce your risk of account takeover fraud by blocking infected links before you ever see them. Initiate transactions from stand-alone PCs that do not allow email or web browsing. Limit the possibility of malware downloaded through links, pop-ups, or attachments.