bank of commerce | bank of choice.

Redding | Sacramento
A division of Redding Bank of Commerce

Customer Education Program

Basic Online Banking Security Best Practices

Online Banking is more secure than ever. Here are some tips and reminders to help keep your account information secure.

- MFA and TAC
    - While our MFA (multi factor authentication) process is one very good way to protect yourself, you can make it even more secure by doing the following:
    - Allow delivery of the TAC (temporary access code) to phones only – Only allow your secure access codes to be delivered via phone, or via text message.
        - NOTE: This is particularly useful in the event that your computer is compromised and you are set up to receive email TAC's. If a criminal has gained access to your online banking credentials they may have access to your email as well.
    - We encourage all of our customers to receive a TAC code at each login (i.e. don't register your computers) - If you force yourself to get a TAC at each login and only allow TAC delivery to phones, this will significantly increase the level of security.
    - Regularly review the secure delivery methods to make sure you have control over each contact. If you see contact methods that do not belong to you - contact the bank immediately
- Alerts
    - All online banking users will be required to receive the following alerts either by phone or text message:
        - Alert me when my login ID is changed
        - Alert me when my password is changed
    - There are also numerous alerts that we encourage all customers to use such as:
        - Alert me when an invalid password for my login ID is submitted
        - Alert me when my security alert preferences are changed
        - Alert me when "forgot password" is attempted for my login ID
    - We may delete any inactive users if not active for a period of 6 months. For security purposes, it is imperative that you do not have inactive users on the system.
    - There are transaction alerts that will notify you when transactions are authorized, cancelled, drafted, processed successfully or failed to process. We encourage all of our customers set up the following:
        - Change of address
        - External transfer
        - Bill Pay
        - Check Reorders
- Passwords
    - Password Complexity - Use complexity measures to strengthen your password using upper case letters, lower case letters, numbers and/or symbols. We recommend that you do not use recurring letters or numbers i.e.: sss or 111 and that you do not use your passwords alternating by a single letter or number 121212 or ababab.

  - Changing your password – We strongly encourage you to change your password often, at least every 90 days.
  - Sharing your password – Do not share your Login ID and password with anyone.
  - Using the same password – We highly recommend that you do not use the same password as you do for your online banking, email and /or any social networking accounts.

- Mobile Banking – If you use our mobile app for iPhone or Android, you are safe and secure.

  - Do not store your passwords on your phone unencrypted.
  - Do not store unencrypted personal information on your phone or any other unsecure application.
  - Critical data should be stored in a digital wallet or password manager with strong encryption, such as 256 bit AES to keep the data safe, secure and accessible.
  - When finished using mobile banking, remember to sign off before accessing another application.
  - If you lose your phone, call your cell phone provider immediately so they can deactivate your phone.
  - If you lose your phone, immediately contact the bank at 800.421.2575 to disable your Login ID and remove your cell phone number for your secure access code delivery method.
  - Utilize the “passcode” or “Auto-lock” options available on your particular device.
  - If available, use the option that will erase or “wipe” your phone after too many unsuccessful passcode attempts.
  - If available, turn on the option to track and remotely erase your device if lost.
  - If you share the device with another user, do not utilize the Touch ID or Face Recognition for mobile banking access as this will allow other users to access your account information.

****Please see our “Mobile Banking Security Best Practices” for additional recommendations.****

- Virus Protection and Computer Safety
  - Virus Protection should be installed with automatic updates, scanning, as well as antispyware software.
  - Never click on a message to install free software.
  - Apply all operating system security patches on an automatic basis to stay current.
  - Ensure that you have a qualified computer technician review your computer at least annually.

- External Transfers
  - All external transfers pass through our security monitoring tool.
  - When a new external account is set up, we have procedures in place to automatically hold the very first outgoing transfer initiated for any dollar amount. We will contact an authorized signer for verification of the validity of this transfer prior to processing the transfer.
  - In addition, any subsequent large dollar outgoing transfer will be held for manual review by our electronic banking support team. If our review identifies this as potentially suspect, we will contact you prior to processing. Otherwise, we will process the transaction without further contact based on your normal transaction history.

  - It is our goal to respond within 15 minutes of a transaction being placed on hold but certain circumstances (i.e. meetings or training sessions) may increase our response time to one hour. As our cutoff time is 5:00 pm PST, external transfers should be submitted by 4:00 pm PST.
  - For your protection, we have established daily and monthly dollar limits for external transfers.

- Logging into Online Banking
  - When you're on our website logging into online banking we will never ask you for:
    - Your name
    - Your date of birth
    - Social Security Number
    - Account number
    - ATM number or PIN
    - If you are ever asked for any of this information at the time of login, STOP and do not login. Chances are you have been redirected to another site.
    - **We will never ask you your password over the phone.**

Lastly, always remember to verify your account activity on a daily basis. Review all transactions prior to our 5:00 pm PST cutoff and contact us immediately at 800.821.2575 if unauthorized transactions appear.