Protection Against Online Fraud in Banking

banking for good

Keep Your Contact Information Up To Date

- Banks can contact you quickly in the event we see suspicious activity on your account
- Travel Plans? Make sure you add travel plans to your online banking. This will allow valid transactions to be approved, and will alert your bank of suspicious activity

Create The Strongest Possible Passwords

- A strong password means a strong defense against hackers
- Utilize password creaters and managers such as those provided standard on Android and Apple devices
- Third party services such as LastPass, NordPass, Keeper and 1Password are great options and can work across platforms

Allow Push Alerts On the Mobile Banking App

- Be alerted of large withdrawals and low account balances to always be aware of what is happening with your accounts
- Banks can contact you quickly in the event we see suspicious activity on your account

Protect Your Devices

- Keeping your phone, tablet and computer up to date with the latest browsers and operating systems helps protect against vulnerabilities that hackers can exploit
- Enable biometrics (fingerprint sign-on or facial recognition)

Know The Red Flags That Signal A Scam

- Payment instructions change last minute
- Overpayment with request to send excess funds back
- Would this entity normally text or email me?
- Craigslist sales and purchases
- Emails or texts about compromised accounts
- Pressuring the sending of money
- Threatening with law enforcement action
- ***When in doubt, always call a publicly posted phone number to confirm instructions/details***

Thank you.