Customer Awareness Program

O'Bannon Bank will NEVER request personal information by email or text messaging including account numbers, passwords, personal identification information or any other confidential customer information.

If you notice suspicious account activity, call our Customer Service Department immediately at (417) 345-2251 to report the suspicious activity.

Tips for keeping your information secure.

- Watch out for suspicious emails that ask for your personal information. If you receive an email from us and are unsure whether it is legitimate, then please contact us and we will be glad to assist you.
- Never give out any personal information including username, passwords, social security number and date of birth.
- Create difficult passwords which include upper- and lower-case letters, numbers, and symbols.
- Don't use personal information for your username or passwords.
- Avoid using public computers to access your online banking.
- Don't give any of your personal information to any website that does not use encryption or other secure methods.

Commercial Banking Security

Perform your own annual internal risk assessment and evaluation on all online accounts.

Establish internal policies regarding employee internet usage.

Ensure all company computers are equipped with up to date antivirus protection software.

Regulation E

Regulation E protects individual consumers engaging in electronic funds transfers (EFT).
Non-consumer (or business) accounts are not protected by Regulation E.

For a complete detailed explanation of protections provided under Regulation E; please visit the Consumer Financial Protection Bureau's (CFPB's) website at www.consumerfinance.gov/eregulations/1005

What is an EFT?

The electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions initiated through electronic-based systems. The term includes, but is not limited to:

- Point of sale transfers
- Automated teller machine transfers (ATM)
- Direct deposits or withdrawal of funds
- Transfers initiated by telephone
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal
- Transfers initiated through internet banking/bill pay

Identity Theft

Identity theft occurs when someone uses your personal information such as your social security number, account number or credit number, without your permission, to commit fraud or other crimes.

How to protect yourself from identity theft.

- Report lost or stolen checks or credit cards immediately.
- Never give out any personal information.
- Never click on suspicious links.
- Shred all documentation that contains confidential information (bank and credit card statements, bills, invoices that contain personal information, expired credit cards and pay stubs).
- Check your credit report annually. www.annualcreditreport.com
- For more information about identity theft visit, www.IdentityTheft.gov

What is Phishing?

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as usernames, passwords and credit card numbers.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a refund
- offer a coupon for free items
- For more information visit, https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams