BANK IMPERSONATION SCAMS ARE ON THE RISE

How It Works

- Fraudsters will contact customers by phone, text, or email claiming to be from the Bank. They will manipulate the account owner into giving away their login credentials, including their Multi-Factor Authentication (MFA) code. Then, they'll use the login credentials to login to the legitimate website and initiate a password reset.
- Additionally, cyber criminals will make fake phishing websites that appear to look like the bank website to trick the account owner into giving away their login credentials. Sometimes, they'll purchase ads that imitate legitimate business ads to increase the prominence of their phishing websites by making them appear more authentic to customers who use a search engine to locate the business' website. When users click the fraudulent search engine ad, they are directed to a sophisticated fraudulent phishing site that mimics the real website, tricking users into providing their login information.
- Once the impersonators have access to the account, they'll quickly wire funds to other accounts, many of which are linked to cryptocurrency wallets. Funds are disbursed quickly and are difficult to trace and recover.

Steps to Spot & Avoid this Type of Bank Fraud

- **Don't rely on caller ID**
  Watch out for scammers who may be able to spoof a phone number so your caller ID reads "Citizens Bank" (or other financial institutions).
- **Never share private account information**
  Remember that your Citizens Bank Banker or other financial institution employees will never contact you and ask for your PIN, password, or one-time access codes. This information should always be protected and not shared with anyone who contacts you.
- **Ignore requests to send a payment to solve a problem**
  Citizens Bank will never ask you to send money to anyone – including yourself – to "reverse a transfer," "receive a refund," "protect your money," or anything similar. Remember, if a correction or new account is needed, the bank will resolve the issue without asking you to make a transfer or withdrawal.
- **Ignore transaction requests you didn't initiate**
  If you receive a one-time access code to authorize a transaction you didn't initiate, don't use the code or share it with anyone, even if they claim to be from your bank. One-time access codes should not be shared.
- **When in doubt, hang up and contact Citizens Bank directly**
  If you receive a suspicious phone call that seems like bank spoofing, hang up immediately. If you receive a suspicious text or email, don't respond. When in doubt, hang up and contact your bank directly.

CITIZENS BANK™
www.citizensEbank.com

Member FDIC
EQUAL HOUSING LENDER

Good Business. Good Friends.