Bank Imposter Scams

EAGLEBANK WILL NEVER ASK YOU FOR YOUR PERSONAL INFORMATION AND PASSWORD

One of the most common fraud scams being perpetuated in the U.S. today involves criminals impersonating bank employees through phone scams and/or message-based deception. The scammers will claim there are urgent or suspicious issues with your account(s) that require immediate attention. Once they have your personal information and identifiers, they can then commit identity theft, open fraudulent accounts, apply for loans, steal your money, and/or engage in other illegal activities.

PHONE SCAMS:

In these scams, the fraudsters will utilize phone calls to impersonate your bank, creating a sense of urgency to trick individuals into divulging sensitive information such as personal identifiers, debit card information and/or account passwords. They may use spoofed phone numbers to contact you where the incoming call appears to be from a legitimate source, adding a layer of believability to these scams. The number you see on caller ID may match your existing bank phone number and the caller may claim there's a security breach, an unauthorized transaction, or another urgent matter, prompting you to disclose personal details or make a payment.

Safeguards:

- Be wary of unsolicited calls; don't rely on caller ID; hang up and call your bank's known/legitimate number
- Protect your personal information; don't share private account information
- Be cautious of any "urgent" requests or notifications of "suspicious activity"
- Ignore transaction requests that you didn't initiate. If you receive a one-time access code to authorize a transaction, don't use the code or share it with anyone, even if they claim to be with your bank.

TEXT/INSTANT MESSAGING/EMAIL SCAMS:

Fraudsters may send messages claiming to be from your bank, and similar to phone scams, often contain urgent messages about account issues, actionable alerts, or enticing offers. These messages may include links to fake websites designed to capture you login credentials or to access your accounts.

Safeguards:

- Avoid clicking on links in unsolicited text messages
- Download and use official banking apps
- Be suspicious of any requests to reset your User ID and Password via a link
- Monitor your accounts

Please report any suspicious EagleBank messages, phone calls or emails to us.

***Note*: EagleBank will never contact you via unsolicited email, text, mail, or phone call asking for sensitive information. If you are suspicious of a call from someone representing themselves as an EagleBank associate, cease contact with them and contact your nearest *EagleBank branch* or call us at 301.986.1800 to report it.**