IMPORTANT REMINDER ON CYBERSECURITY AND TIPS ON HOW TO RECOGNIZE AND AVOID PHONE CALL & PHISHING SCAMS

The federal government has issued an advisory on the need for heightened cybersecurity given the current unrest in the Urkraine. Please be on the alert for phishing scams attempting to trick you into providing your account or personal identifying information. **Pan American Bank and Trust will never call, email or text you with a request to provide such information.**

How To Recognize a Phone Scam

While you may occasionally receive a phone call from a Pan American Bank & Trust representative, we will never ask you to disclose or verify sensitive personal information or an account number. If you are asked to provide this information, hang up and call us using the phone number on your account statement to report the suspicious call.

How To Recognize Phishing

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store. **Never click on a link in a text or email to call the bank or credit card company. Call the bank or credit card company directly using the phone number on your account statement.**

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 government refund
- offer a coupon for free stuff

How To Protect Yourself From Phishing Attacks

- **Protect your computer by using security software**. Set the software to update automatically so it can address any new security threats.
- **Protect your mobile phone by setting software to update automatically.** These updates could give you critical protection against security threats.
- **Protect your accounts by using multi-factor authentication.** Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password. The additional credentials you need to log in to your account fall into two categories:
    - Something you have — like a passcode you get via an authentication app or a security key.
    - Something you are — like a scan of your fingerprint, your retina, or your face.

- **Protect your data by backing it up.** Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.