October 2023

CYBERSECURITY NEWSLETTER

Pegasus Protects.

Pegasus BANK

20 Years of Cybersecurity Awareness Month!

Since 2004, the National Cybersecurity Alliance and the Cybersecurity and Infrastructures Agency (CISA) have collaborated with government and private industry to raise awareness about digital security and to empower everyone to protect their personal data from digital forms of crime.

This year we are focusing on four key behaviors:

- **Enabling multi-factor authentication**
- **Using strong passwords and a password manager**
- **Updating software**
- **Recognizing and reporting phishing**

Enable Multi-factor Authentication

Multi-factor authentication (MFA) is a security technology that requires multiple methods of authentication for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token or one time code; and what the user is, by using biometric verification. According to industry research, users who enable MFA are up to 99% less likely to have an account compromised.

Most platforms offer additional layers that can be used during login. Visit the sites' settings area to see what is offered. We encourage MFA to be enabled on all bank, brokerage, utility, phone, retail and primary computer logins.

Use a password manager from strong, unique passwords

The keys to your digital castle are your passwords. You want to take every precaution to keep your passwords secure, just like you would with your house keys. All passwords should be generated with the following three guiding principles in mind, regardless of the accounts they protect:

- **Long –** At least 12 characters should be included in each of your passwords.
- **Unique –** Each account must be secured by a separate, individual password.
- **Complex –** Each password should be complex and contain a mix of capital and lowercase letters, digits, and special characters.

A password manager provides the easiest approach to establish and maintain strong passwords for the growing number of online accounts you connect into. Not only will a password manager store hundreds of different passwords; it can also alert you when a password has been compromised, warn of possible phishing sites, and work across all of your operating systems and devices.

Always Update Your Software

Keeping your software and apps updated is one of the simplest ways to keep your information secure. Software updates are a simple method to stay one step ahead of the bad guys by closing any known vulnerabilities.

To more easily stay on top of your updates, consider automating the process. The option to automatically update your program is typically offered by software from reputable vendors. It provides a notification when an update is available so you can start the process right away.

Recognizing and Reporting Phishing

Cyber criminals use targeted e-mails, text messages, and even phone calls that appear to come from a trustworthy source. The goal is to steal sensitive data like credit card and login information or to install malware onto the victim's machine. In some cases, the attack can start as a text message and move to a phone call if you acknowledge the message.

As a reminder, Pegasus Bank will never contact you and ask that you provide your debit card number, online banking login ID, or online password. Many fraudsters use generic terms such as **"Fraud Center"** to make you feel as though they are legitimate. If you are unsure about the person on the phone, please hang up and contact Pegasus Bank directly at: **214-353-3000**.

Modern Day Scammers Utilizing Artificial Intelligence to Execute Sophisticated Attacks

It's the phone call every parent dreads: a voice on the other end claiming to be their child, now kidnapped or arrested, pleading for help. While such scams have been in existence for years, the game has changed considerably with the introduction of AI-driven voice mimicry. In these scenarios, threat actors use cutting-edge artificial intelligence to impersonate the voice of a loved one, making the scam all the more convincing and emotionally wrenching for the unsuspecting victim.

Why Voice Mimicry is Effective

1. **Emotional leverage –** When victims hear what they believe to be their child's voice, they often react emotionally rather than rationally. This can lead to quick, impulsive decisions like transferring money without verification.
2. **Bypassing Skepticism –** The human mind associates voice with identity. When the voice matches expectations, it bypasses many of the usual skeptical questions and red flags that might arise from a written message or unfamiliar voice.

In typical ransom scams, attackers claim that they've kidnapped the victim's child and demand money for their release. With voice mimicry, this scam's believability is significantly enhanced as the 'child' can now directly speak to the parent, pleading for assistance.

Similarly, in bail scams, the caller, posing as an arrested child, might request funds to post bail or hire a lawyer. Again, hearing their child's voice escalates the urgency and reduces the parent's suspicions.

Protecting Yourself and Your Loved Ones

1. **Awareness –** Simply being aware of this technology and its malicious use can prevent one from falling victim. Always approach such calls with caution.
2. **Verification –** No matter how convincing the voice is, always verify the situation. If your child is supposedly arrested, call the police station or your child's last known location. For a kidnapping claim, try reaching your child on their personal phone or through other means.
3. **Pre-set code words –** Establish a family emergency code word. If a genuine emergency arises, the use of this code word can quickly confirm with legitimacy of the situation.

As technological advancements continue, the tactics employed by scammers will become more sophisticated. However, by staying informed and maintaining a healthy level of skepticism, individuals can protect themselves from falling prey to such emotionally manipulative scams.

Disclaimer: This article was written by Chat GPT.

Need Help? Contact Pegasus Bank's **Treasury Management team** at **(214) 353-3085** or email us at: **tm@pegasusbankdallas.com**.