Legence Bank Member FDIC

04/14/2023: AI Fraud on the Rise

Artificial Intelligence (AI) has made our lives easier and more efficient in many ways, but it has also created new opportunities for fraudsters to exploit unsuspecting victims. Impersonation scams are a popular form of AI fraud that can be particularly convincing and dangerous. Scammers are using AI technology to mimic the voice or identity of someone you know, such as a loved one or a trusted organization, in order to trick you into giving them money or personal information.

Here are some quick tips that can help you avoid falling victim to AI impersonation scams:

- **Verify the Identity of the Caller:** If someone calls claiming to be a friend or family member, ask them questions that only that person would know, such as their favorite color or hobby. Avoid asking questions that could be answered easily by online research. Another popular option is agreeing on a codeword that would be used in conversation to help loved ones recognize one another. Often, scammers are not prepared to answer those questions and would not be able to provide a private codeword to verify their identity.

- **Don't Be Rushed:** Scammers often create a sense of urgency to pressure you into giving them money or information. If someone contacts you demanding immediate payment or is threatening you in any way, it's likely a scam. Scammers often play on emotion in hopes that potential victims will act quickly without thinking clearly. Slow down. Take your time and verify their identity and the situation before taking any action.

- **Hang Up and Call Back:** If someone is claiming to be from a trusted organization, hang up and call them back using a number that you know for certain is legitimate. This will help confirm if the call originated from a fraudster or was legitimate. Do not trust Caller ID. Fraudsters are able to easily spoof phone numbers when making outbound calls but are usually unable to receive inbound calls to the same number.

- **Keep Personal Information Private:** Be wary of sharing any personal information over the phone, via text, messaging app, or email, especially if you didn't initiate contact. Unsolicited calls and messages often lead to scams involving identity theft and monetary loss.

- **Educate Yourself:** Learn about the different types of impersonation scams and how you can spot them. AI fraud is unfortunately on the rise. Remember, prevention is key when it comes to any type of fraud. By staying vigilant and taking steps to protect your personal information, you can help keep yourself and your loved ones safe from these scams and others.

This type of scam was demonstrated in a very recent case where a daughter was supposedly kidnapped, and fraudsters attempted to trick her mother into sending them a large sum of money. This is just one example of the many ways that fraudsters use AI to create convincing and emotionally manipulative scams. Click the link below for the full story from the New York Post:

https://nypost.com/2023/04/12/ai-clones-teen-girls-voice-in-1m-kidnapping-scam/