Public Service Announcement

Federal Bureau of Investigation

December 12, 2024

Scammers Target Potential Financial Victims With Texts

The Federal Bureau of Investigation (FBI) in Louisiana warns the public of a fraudulent scheme in which scammers impersonate bank representatives, hereinafter “impersonators,” to fraudulently obtain information giving them access to bank customers’ accounts.

HOW THE SCHEME WORKS

Bank customers receive a text message that appears to be from their financial institution, asking if they have authorized a transaction. The message asks the individual to reply “yes” or “no” or to “opt out”. When the customer responds, they receive another message indicating the “bank” will contact them shortly. The impersonators then call the customer from a number that appears to be from a financial institution (spoofing) asking for account, online banking, and other personal identifying information. With that information, the impersonators have called legitimate financial institutions and changed account information without the legitimate customer’s consent, giving the fraudsters access and control to the account.

HOW TO PROTECT YOURSELF

- RESIST the pressure to act quickly. DO NOT respond to texts asking for personal information or confirm transactions or other account activity.
- Do not respond to unexpected emails about unsolicited services or services you did not purchase.
- When in doubt, search online for accurate financial institution information and initiate the communication from your end. If you are called by someone claiming to be an official institution, look up the contact information, and call back. If possible, visit your financial institution in person.
- Do not provide banking or personally identifiable information (date of birth, social security numbers, addresses) via text, email or by telephone. These can be used to open or change credit or banking accounts without your consent.

If you believe you have been a victim of a financial fraud scheme, please file a report with the FBI's Internet Crime Complaint Center at www.ic3.gov. If possible, include the following:

- Identifying information about the individuals including name, phone number, address, and email address.
- Financial transaction information such as the date, type of payment, amount, account numbers involved, the name and address of the receiving financial institution, and receiving cryptocurrency addresses.
- Describe your interaction with the individual, including how contact was initiated, such as the type of communication, purpose of the request for money, how you were told or instructed to make payment, what information you provided to the scammer, and any other details pertinent to your complaint.