Impersonation Scams

How they work and how to identify the signs

FRAUD PREVENTION

Impersonation scams, sometimes referred to as imposter scams, are one of the most common types of scams. These types of scams involve fraudsters contacting their victims via text message, phone call, or email, and posing as a commonly known business, financial institution, or government agency. The text messages, emails, and phone calls used to initiate these scams typically state that there is some sort of issue with an account, subscription, etc. Fraudsters work to convince victims that in order to resolve the issue, the victim needs to comply with the fraudster's instructions. The instructions commonly involve making a payment, sending funds, or sharing account or card details. The "representative" will ask victims to provide personal information that they claim is used to verify the victim's identity.

It is important to be vigilant when answering phone calls, text messages, and emails from unknown numbers or emails posing as businesses, financial institutions, and government agencies. As technology advances so is the methodology used by fraudsters to carry out these scams. Fraudsters have gone as far to alter the caller ID on phone calls to appear as a legitimate business number with the name and number matching whatever business or government agency they are posing as. This is misleading and makes it easy for scams to be carried out.

Resources

usa.gov: Imposter Scams
ftc.gov: Impersonation scams-not what they used to be
bbb.org: Impersonation Scams

How to Protect Yourself from Becoming a Victim of an Impersonation Scam

- Slow Down – When reviewing an incoming text message or email and answering an unexpected phone call, take a moment to verify the information the caller is telling you. Acting on impulse is often why many of these schemes are successful. Use your resources to verify the information they provide: conduct online research and request a call back phone number to contact them back after reviewing the situation and details. Compare the call back number given with the phone numbers listed on the business or government agencies' websites, or in the case of a financial institution, the phone number listed on the back of your debit card / credit card. It is always helpful to get a second opinion from a trusted family member or friend on the situation. When in doubt, call the business or agency directly using the phone number available on their website to inquire if they called you.
- Be Reasonable – If someone unexpectedly contacts you demanding money, personal information, or banking information urgently, chances are it is a scam. Fraudsters will often request that you make a wire transfer, gift cards, or cryptocurrency in order to resolve whatever issue they claim you are having. Do not comply with their requests. Along the same lines, your financial institution will not call you requesting that you provide sensitive personal or banking information such as your account number, social security number, or PIN number. In these situations, it is best to hang up and call your financial institution to verify that it was not them attempting to contact you.
- Stay Calm – Fraudsters frequently use scare tactics to pressure their victims into acting urgently. It is important to stay calm and remember that a legitimate business or government agency would not pressure you to act in a hasty and rushed manor. Your financial institution is a great resource in these situations and can assist you with identifying scams before you fall victim to a scheme.