BankOnITUSA®

INFORMATION SECURITY BRIEF

MARCH 2023

IRS RELATED SCAMS

Tax time is upon us, a sign that phishing season has begun. In the next two editions of the Information Security Brief, we'll cover some tax-related scams and expose common lures used by criminals to look and sound more legitimate.

The IRS states that scams may differ in themes, but generally, they have two traits:

- They appear to come from a known or trusted source, such as a colleague, bank, credit card company, cloud storage provider, tax software provider, or even the IRS.
- They tell a story, often with an urgent tone, to trick the receiver into opening a link or attachment.

VISHING (Phone Phishing)

Criminals continue to make aggressive calls posing as IRS agents in hopes of stealing money or personal information. A method you can use to identify IRS Vishing is to know what the IRS will never do. The IRS informs us that they will never do the following:

- Call to demand immediate payment using a specific payment method, such as a prepaid debit card, gift card, or wire transfer. Generally, the IRS will mail a bill to taxpayers who owe taxes.
- Threaten immediately bringing in local police or other law enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without allowing taxpayers to question or appeal the amount owed.
- Call unexpectedly about a tax refund.

It doesn't need to be tax time for a Vishing scam to be used. Victims have reported receiving calls from a familiar number, such as their bank. The scammers will tell the victim that their account was compromised, and they will need to verify the account with the victim's personal information.

The scammer may also direct the victim to a website and download software that would spy on the victim or give the scammer remote access to your computer.

HOW TO AVOID A SCAM

- Block unwanted calls or text messages.
- Don't give your personal or financial information in response to a request you didn't expect.
- Resist the pressure to act immediately.
- Know how scammers tell you to pay. You should never have to pay for a legitimate business with cryptocurrency, a wire transfer service, or a gift card. Further, never deposit a check sent to you and send money back to the solicitor (scammer).
- Stop and talk to someone you trust.