Money Talks March 2023

By David Helscher

With income tax filing season underway, this is the prime period for fraudsters to hit people with realistic-looking emails, texts, and phone calls. The IRS is reminding taxpayers to use caution and avoid becoming the victim of a fraudulent tax scheme. Last year there was an increase in text messages sent to smartphones by persons impersonating the IRS. Below are some of the most common tax scams to watch out for.

Phishing scams usually involve unsolicited emails or text messages that seem to come from legitimate IRS sites to convince you to provide personal or financial information. Once scam artists obtain this information, they use it to commit identity or financial theft. The IRS does not initiate contact with taxpayers by email, text message, or any social media platform to discuss personal tax issues, such as bills or refunds. The IRS initiates most contacts through regular mail delivered by the US Postal Service.

Phone scams typically involve a phone call from someone claiming that you owe money to the IRS or you're entitled to a large refund. The calls may show up as coming from the IRS on your caller ID, be accompanied by fake emails that appear to be from the IRS, or involve follow-up calls from individuals saying they are from law enforcement. These scams often target more vulnerable populations, such as immigrants and senior citizens, and will use scare tactics such as threatening arrest, license revocation, or deportation. Criminals can fake or "spoof" caller ID numbers to appear to be anywhere in the country, including an IRS office, local law enforcement, or state or federal agencies.

Tax-related identity theft occurs when someone uses your Social Security Number to claim a fraudulent tax refund. You may not even realize you've been the victim of identity theft until you file your tax return and discover that a return has already been filed using your Social Security Number. Or the IRS may send you a letter indicating it has identified a suspicious return using your Social Security Number. To help prevent tax-related identity theft, the IRS now offers the Identity Protection PIN Opt-In Program. The Identity Protection PIN is a six-digit code that is known only to you and the IRS, and it helps the IRS verify your identity when you file your tax return.

Other scams can take the form of a fake offer in compromise to help settle a tax debt. Another scam is to pose as a legitimate charitable organization to solicit donations, taking advantage of tragedies, disasters, or conflicts. Before donating to a charity, make sure it is legitimate and never donate cash, gift cards, or funds by wire transfer.

There are some things you can do to help protect yourself from scams, including those that target taxpayers. Don't click on suspicious or unfamiliar links in emails, text messages, or IM services. Don't answer a phone call if you don't recognize the phone number, let it go to voice mail and check later to verify the caller. Never download email attachments unless you can verify that the sender is legitimate. Keep device and security software up-to-date and maintain strong passwords. Never share personal or financial information via email, text message, or over the phone.