February, 2017
Volume 12, Issue 2

Staying Safe From Tax Season Scams

The Henry County Bank

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

Now that W-2's are arriving, it's time to consider how to stay safe from tax season scams. Every year, unfortunate taxpayers go to file their returns and are shocked to find that someone else has filed a fraudulent one in their name! Some innocent people also receive fraudulent phone calls from criminals impersonating tax officials. Sadly, tax fraud has only become more widespread and digital communication has opened new ways for it to happen.

While the Internal Revenue Service (IRS) reports on multiple tax-payer related scams, and even publishes a "Dirty Dozen" list[1], three scams variants are worth highlighting: Phishing and Malware Schemes; Identity Theft and Falsely Filed Tax Returns; and Impersonation Scams. Once criminals have your information, they can also continue to commit identity theft well beyond tax season. Here are some details on each of these scams, along with how to identify them and seek help in case of identity theft.

Phishing and Malware Schemes:

The first type of scam often leads to identity theft and falsely filed tax returns, but may also result in you downloading malware. This happens when criminals send convincing phishing emails or direct you to convincing websites that appear to be IRS, state government, tax software, or financial institution websites. Their goal is to trick you into entering your login credentials, verifying sensitive personal information, or downloading malware.

- *Never click on email links; type the organization's website into your web browser.*
- *If you feel something is suspicious, contact the organization through a known method, like their publicly-posted customer service line.*
- *Do not reply to emails or texts asking for personal or tax information.*

Identity Theft and Falsely Filed Tax Returns:

Once criminals have your personal information, they can use it to commit identity theft or file a false tax return in your name. In this case, if the criminal files the return before you do, they are getting your refund money and forcing you to go through the arduous process of proving that it was not you who filed the return. Criminals send phishing emails or make phone calls to trick you into providing your information so that they can commit this type of fraud.

- *Be wary of any contact by phone or email claiming to be from the IRS, as they do not contact taxpayers directly for this type of information.*
- *File your tax return as soon as you get your W-2's and other tax information. Criminals cannot successfully file a fraudulent return if you have already filed with the IRS!*

[1] https://www.irs.gov/uac/newsroom/dirty-dozen

Impersonation Scams:

Our final flavor of scam involves a criminal impersonating the IRS or a tax official, such as a tax advocacy panel or tax preparer. They may say you owe money to the IRS or your state tax department or may represent themselves as a trusted tax authority and request information. This contact can occur through websites, emails, or threatening calls or text messages, that seem official. Sometimes, these scammers request that their victims pay by strange methods like gift cards or pre-paid credit cards.

If you do in fact owe tax money to the IRS, you will receive an official bill in the mail first before being contacted by phone or email. For a quick reference, the IRS states that these are four things they will never do:[2]

- *ask for credit or debit card numbers over the phone;*
- *call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer;*
- *threaten to immediately bring in local police or other law-enforcement groups to have you arrested for not paying;*
- *demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.*

Seeking help and reporting scams:

The IRS encourages taxpayers to send suspicious emails related to tax fraud to its phishing@irs.gov email account. Other forms of tax fraud can be reported by following the instructions here: https://www.irs.gov/Individuals/How-DoYou-Report-Suspected-Tax-Fraud-Activity%3F.

If you suspect that you have been a victim of fraud or identity theft, please head to https://www.identitytheft.gov/. This is a site run by the Federal Trade Commission that provides a step-by-step recovery plan and assistance in taking action. It allows you to report if someone filed a return fraudulently in your name, if your information was exposed in a major data breach, and in case of many other types of fraud. If you believe you someone has used your social security number to fraudulently submit a tax return, you can also call the IRS at 800-908-4490.

Keep these common types of fraud in mind, and don't hesitate to seek assistance if you become a victim.

[2] https://www.irs.gov/uac/tax-scams-consumer-alerts