February 2019
Volume 14, Issue 2

Staying Safe from Tax Scams

Mendee L. Wyenandt, CIO
6415 Bridgetown Road
Cincinnati, Ohio 45248
513-574-0700

From the desk of *Mendee L. Wyenandt*

As people seek to file their tax returns this year, cybercriminals will be busy trying to take advantage of this with a variety of scams. Citizens may learn they are victims only after having a legitimate tax return rejected because scammers already fraudulently filed taxes in their name. According to the Internal Revenue Service (IRS), there was a 60% increase in 2018 in phishing scams that tried to steal money or tax data. The IRS identified 9,557 fraudulent tax returns as of only February 24th, 2018 for the last filing season. As everyone aims to file their returns among all this fraud, the following advice will explain how tax fraud happens and provide recommendations on how to prevent it from happening to you or how to get help if you are unfortunately affected by a tax scam!

How is tax fraud perpetrated?

The most common way for cybercriminals to steal money, financial account information, passwords, or Social Security Numbers is to simply ask for them. Criminals will send phishing messages often impersonating government officials and/or IT departments. They may tell you a new copy of your tax form is available. They may include a link in a very official looking email that goes to a website that uses an official organization's logo and appears legitimate, yet is fraudulent. If you attempt to login into the false website, or provide any personal information, the criminals will see what you type and try to use it to compromise your other accounts and file a false return in your name.

Additionally, much of your personal information can be gathered online from sources like social media or past data breaches. Criminals know this, so they gather pieces of your personal information from a variety of sources and use the information to file a fake tax refund request! If a criminal files a tax return in your name before you do, you will go through the arduous process of proving that you did not file the return and subsequently correcting the return.

Criminals also impersonate the IRS or other tax officials, demanding tax payments and threatening you with penalties if you do not make an immediate payment. This contact may occur through websites, emails, or threatening calls or text messages that seem official but are not. Sometimes, criminals request their victims to pay "penalties" via strange methods like gift cards or prepaid credit cards. It is important to remember that the IRS lets citizens know it *will not* do the following:

- Initiate contact by phone, email, text messages, or social media without sending an official letter in the mail first.
- Call to demand immediate payment over the phone using a specific payment method such as a debit/credit card, a prepaid card, a gift card, or a wire transfer.

- Threaten you with jail or lawsuits for non-payment.
- Demand payment without giving you the opportunity to question or appeal the amount they say you owe.
- Request any sensitive information online, including PIN numbers, passwords or similar information for financial accounts.

How can you protect yourself from tax fraud?

- File your taxes as soon as you can…before the scammers do it for you!
- Always be wary of calls, texts, emails, and websites asking for personal or tax data, or payment. Always contact organizations through their publicly-posted customer service line. If they contact you end the call and call the organization on the phone number on their website. As mentioned previously, the IRS will initiate contact on these issues by mail through the postal service.
- Don't click on unknown links or links from unsolicited messages. Type the verified, real website address into your web browser.
- Don't open attachments from unsolicited messages, as they may contain malware.
- Only conduct financial business over trusted sites and networks. Don't use public, guest, free, or insecure Wi-Fi networks.
- Use strong, unique passwords for all your accounts and protect them. Reusing passwords between accounts is a big risk that allows a breach of one account to affect many of them!
- Shred all unneeded or old documents containing confidential and financial information.
- Check your financial account statements and your credit report regularly for unauthorized activity. Consider putting a security freeze on your credit file with the major credit bureaus. This will prevent identity thieves from applying for credit or creating an IRS account in your name.

If you receive a tax-related phishing or suspicious email at work, report it according to your organization's cybersecurity policy. If you receive a similar email on your personal account, the IRS encourages you to forward the original suspicious email *as an attachment* to its phishing@irs.gov email account, or to call the IRS at 800-908-4490. More information about tax scams is available on the IRS website and in the IRS Dirty Dozen list of tax scams.

If you suspect you have become a victim of tax fraud or identity theft, the Federal Trade Commission (FTC) Identity Theft website provides a step-by-step recovery plan. It also allows you to report if someone has filed a return fraudulently in your name, if your information was exposed in a major data breach, and many other types of fraud.

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™