March 2018
Volume 13, Issue 3

Staying Safe from Tax Scams

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

Though Benjamin Franklin is often quoted as saying "in this world, nothing can be said to be certain, except death and taxes," an updated version for the current day would need to include tax scams. As people nationwide seek to file their tax returns, cybercriminals attempt to take advantage of this with a variety of scams. Hundreds of thousands of U.S. citizens are targeted by tax scams each year, often only learning of the crime after having their legitimate returns rejected by the Internal Revenue Service (IRS) because scammers have already fraudulently filed taxes in their name. The IRS reported a 400% rise in phishing scams from the 2015 to the 2016 tax season. In the state, local, tribal, and territorial government sector during 2017, approximately 30% of all reported data breach incidents were related to the theft of W-2 information, which was likely used for tax fraud.

How is Tax Fraud Perpetrated?
Unfortunately, much of your personal information can be gathered from multiple locations online with almost *no verification* that the right person is receiving the information. Criminals know this, so they use this trick to get your personal information from a variety of websites and use the information to file a fake tax refund request! If a criminal files a tax return in your name before you do, they will file it with false information to get a large refund, forcing you to go through the arduous process of proving that you did not file the return and subsequently correcting the return. Once they have your personal information, criminals can continue to commit identity theft well beyond the tax season.

Another way criminals gather your information is through the W-2 variant of the Business Email Compromise scam. Criminals using this scam trick others into providing your personal information.

Another favorite technique used by criminals during the tax season is sending phishing messages indicating that a new copy of your tax form(s) is available. These emails often impersonate state, local, tribal, and territorial government comptroller and/or IT departments. They might include a link to a phishing website that uses your organization's logo and the email might even have the right signature line. If you fill out or attempt to login into the phishing website, the criminals will be able to see your login name and password, which they can then use to try and compromise your other accounts. The more information they gather from you, the easier it is for them to use the information to file a fake tax return in your name.

Tax fraudsters also impersonate the IRS and other tax officials to threaten taxpayers with penalties if they do not make an immediate payment. This contact may occur through websites, emails, or threatening calls and text messages that look official but are not. Sometimes, criminals request their victims pay the "penalties" via strange methods like gift cards or prepaid credit cards. It is important to remember:

- The IRS will not initiate contact about payment with taxpayers by phone, email, text messages, or social media without sending an official letter in the mail first.

- The IRS will not 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.
- The IRS will not threaten to immediately notify local police or other law-enforcement agencies to have you arrested for not paying.
- The IRS will not demand that you pay taxes without giving you the opportunity to question or appeal the amount you owe.

What Can You Do?

Here are some basic tips to help you minimize the chances of becoming a victim of a tax scam:

- If you haven't already, file your taxes as soon as you can…before the scammers do it!
- Be aware of phone calls, emails, and websites that try to get your information, or pressure you to make a payment. If something seems suspicious, contact the organization through a known method, like their publicly posted customer service line.
- Ignore emails and texts asking for personal or tax information. Be cautious as to whom you provide your information, including your Social Security Number and date of birth.
- Don't click on unknown links or links from unsolicited messages. Type the verified, real organizational website into your web browser.
- Don't open attachments from unsolicited messages, as they may contain malware.
- Only conduct financial business over trusted websites. Don't use public, guest, free, or insecure Wi-Fi networks.
- Remember, the "HTTPS" does not mean a site is legitimate.
- Shred all unneeded or old documents containing confidential and financial information.
- Check your credit report regularly for unauthorized activity. Consider putting a security freeze on your credit file with the major credit bureaus if you suspect you have been targeted for identity theft.

If you receive a tax-related phishing or suspicious email at work, report it according to your cybersecurity policy. The IRS encourages taxpayers to send suspicious emails related to tax fraud 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 will provide a step-by-step recovery plan. It also allows you to report if someone has filed a tax return fraudulently in your name, if your information was exposed in a major data breach, and many other types of fraud.