Monthly Cybersecurity Newsletter

February 2019 Issue

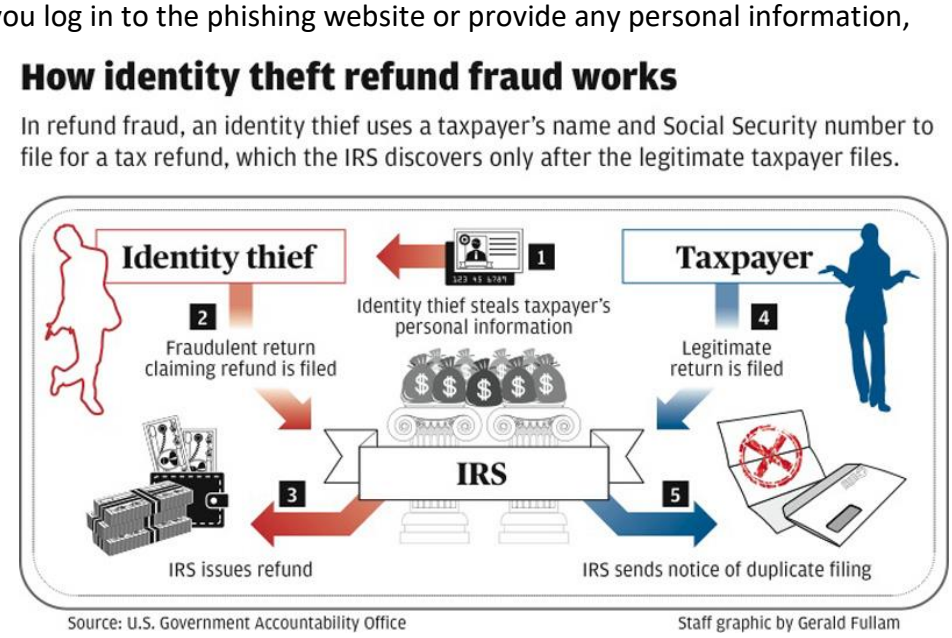
Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

Staying Safe from Tax Scams!

As people nationwide will file their tax returns this year, cybercriminals will be busy trying to take advantage of taxpayers with a variety of scams. Every year, tax scams affect hundreds of thousands of U.S. citizens, who usually learn of the crime after their legitimate returns are rejected because scammers have already fraudulently filed taxes in their name. According to the Internal Revenue Service (IRS), phishing scams designed to steal money or tax data increased **60 percent** in 2018. The IRS received more than 2,000 tax-related scam reports from January to October 2018, compared to just 1,200 incidents in all of 2017. In 2017, more than 200 employers were victims of W-2 scams, compromising the identities of hundreds of thousands of employees.

Criminals conduct tax scams in several ways. Most commonly, cybercriminals simply *ask* for your money, financial account information, passwords, or Social Security numbers. Criminals send you phishing messages often impersonating state, local, tribal, and territorial government officials and/or IT departments. They might tell you that a new copy of your tax form(s) is available. They may include a link in a phishing email that goes to a website that uses an official organization's logo. If you log in to the phishing website or provide any personal information, the criminals will see it, and then try to use it to compromise your other accounts. The more information they gather from you, the easier it is for them to use it to file a fake tax return in your name. Criminals may even embed malware into tax-related documents and send those via email to unsuspecting victims.



Criminals also like to impersonate the IRS or other tax officials, demanding your money **now** 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 the IRS 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 will jail or lawsuits for not paying.
- ⃠ 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?

Here are some ways you can lessen the risk of becoming a victim of a tax scam:

- File your taxes as soon as you can, before scammers do it for you!
- Be aware of phone calls, emails, and websites that try to get your personal or tax data, or pressure you to make a payment.
- Ignore emails or texts asking for personal or tax information.
- Don't click on unknown links or links from unsolicited messages. Type the verified, real organization's 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 for financial business.
- Don't trust the "HTTPS" in the web address to mean a site is legitimate.
- Use strong, unique passwords for all your accounts and protect your passwords.
- Shred all unneeded or old documents containing confidential and financial information.
- Check your financial account statements and your credit report regularly. Consider putting a security freeze on your credit file with the major credit bureaus. This will prevent criminals 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 agency's cybersecurity policy. If you receive a similar email on your personal account, the IRS encourages you to forward the original suspicious email (*with headers or as an attachment*) to phishing@irs.gov, 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.

TAX SEASON GOT YOU FLUSTERED?

Follow these simple steps:

- ☐ File your taxes as early as possible.
- ☐ Protect your personal information.
- ☐ Keep your computer secure and up-to-date.
- ☐ Don't fall for phony threats or requests for information.

Business Email Compromises (BEC)

The Multi-State Information Sharing and Analysis Center (MS-ISAC) recently distributed a warning about Business Email Compromise (BEC) scams. BEC scams attempt to deceive victims into sending money, or personally identifiable information (PII), or attempt to deceive victims into modifying direct deposit information. Criminals target organizations in order to cause data breaches, resulting in financial fraud or identity theft. A BEC commonly happens in this way: a cybercriminal gains access to the email address of a senior executive in an organization or spoofs the executive's email address. The cybercriminal then sends requests for money or information to employees of the organization who trust that senior executive. Indicators of BEC spam emails can include the following:

- ✓ Poorly crafted emails with spelling and grammar mistakes.
- ✓ An incorrect or abbreviated signature line for the supposed sender.
- ✓ The use of full names instead of nicknames, and a language structure that may not match how the supposed sender normally communicates.
- ✓ The only way to contact the sender is through email.
- ✓ The transactions are for a new vendor or a new contact at a known vendor.

What can you do about BEC threats? Everyone needs to play the role of ***Human Firewall***!

- ❖ Treat requests for money or sensitive information with a high degree of skepticism.
- ❖ Always follow your organization's policies and procedures.
- ❖ Stay alert for anything that seems out of the ordinary.
- ❖ If you're not sure about a request, please ask! There are no stupid questions.

>>>Monthly Newsletter

Don't forget the following resources available to you. The following are some other **cybersecurity newsletters** the ESRMO recommends. We hope you find them beneficial and share them with your peers!

Security Awareness Newsletter: A monthly security awareness newsletter that is provided by KnowBe4 for all State employees. ***Note****: You must have a valid State employee O365 account.*

- ➢ https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). The topic this month is ***How to Stay Safe from Tax Scams***.

- ➢ https://www.cisecurity.org/resources/newsletter

SANS OUCH! Newsletter: A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Personalized Scams.***

- ➢ https://www.sans.org/security-awareness-training/ouch-newsletter

The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link:

https://www.sans.org/security-awareness-training/video-month

The SANS Institute free webcasts may be accessed via the following link:

https://www.sans.org/webcasts/upcoming.

Coalfire, a PCI compliance validation services vendor, will be hosting a one-hour webinar for the State of NC's merchant community on **March 5, 2019, at 10 a.m**. Information regarding the webinar is provided below:

Webinar Title: PCI Scope Impacts from Using P2PE or Other Non-listed Encryption Solutions

Webinar Description: Merchants recognize that using payment encryption can increase the security of a retail environment, but often misunderstand the resulting impacts to merchant PCI DSS scope. In this webinar, many types of payment encryption technologies will be reviewed, including P2PE, NESA, and other non-listed encryption solutions offered by processors, gateways, POS vendors, and other solution providers. By better understanding the terminology, differences between these types of solutions, guidance from the PCI Security Standards Council, and how QSAs approach this topic, attendees will be better prepared to select, implement, and maintain solutions that provide the greatest security, compliance, and value.

Webinar Credentials: Join from your computer or mobile: https://fuze.me/95138164

Call in information:

- 201-479-4595 (toll) or (855) 346-3893 (toll free)
- Enter the meeting ID 95138164 followed by the # key

Speaker: Sam Pfanstiel is a Senior Consultant for P2PE within the Payments Assurance practice at Coalfire. In this role, he is responsible for providing consulting and assessment services for P2PE solutions and components and identifying the impacts of cryptographic solutions on merchant payment environments. Mr. Pfanstiel joined Coalfire in 2016, with two decades of senior IT management and payments security experience. His experience covers a broad spectrum of disciplines, including payment security, PCI compliance, card brand compliance, fraud, application security, mobile security, IT infrastructure, software development, and P2PE. While at Coalfire, Sam has focused primarily on P2PE and PCI solution architecture, business analysis, cryptosystem review, and performing PCI DSS and P2PE workshops and assessments.

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.