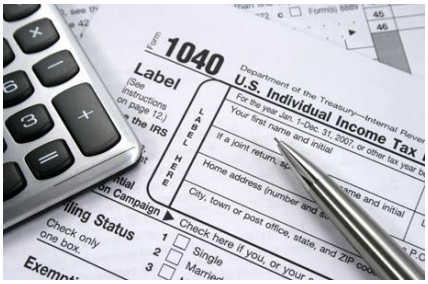
Monthly Cybersecurity Newsletter

February 2018 Issue

Enterprise Security and Risk Management Office (ESRMO)

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

Be Aware of Tax Scams!



It is everyone's favorite time of year - tax season – and people are working on getting their taxes done for the State and for Uncle Sam. This is also the time when cybercriminals take advantage of people with tax scams. Tax scams affect hundreds of thousands of U.S. citizens each year, who usually learn of the crime after having their returns rejected because scammers beat them to it. The Internal Revenue Service (IRS) reported a 400% rise in phishing scams from the 2015 to the 2016 tax season. Reports to the IRS from victims and nonvictims about W-2 scams jumped to approximately 900 in 2017, compared to slightly over 100 in 2016. Last year, more than 200 employers were victimized with W-2 scams, which meant hundreds of thousands of employees had their identities compromised.

Criminals conduct tax scams in several ways. They can get your personal information from a variety of third-party and government websites and then file a fake tax refund request! They can also get your personal information from fake websites that trick you into entering your login credentials, your personal information, or downloading malware onto your computing device. Criminals may embed malware into tax related documents and send those via email to unsuspecting victims. They may even impersonate the IRS or other tax officials and threaten you with arrest, deportation or other penalties if you do not make an immediate payment. This contact can occur through websites, emails, or threatening calls or text messages that may seem legitimate. Criminals often request victims to pay by strange methods like gift cards or prepaid credit cards. It is important to remember that the IRS will not do the following:

- Initiate contact with taxpayers by phone, email, text messages, or social media without sending an official letter in the mail first.
- 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 to immediately notify law-enforcement to have you arrested for not paying.
- Demand you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.

The IRS requests taxpayers send suspicious emails related to tax fraud to phishing@irs.gov.

So, what can you do to minimize the chances of becoming a victim of a tax scam?

- File your taxes as soon as you can…before the bad guys do it for you! You can minimize the chance of tax refund fraud by filing your taxes early.
- Be aware of phone calls, emails, and websites that try to get your personal or tax data, 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.
- Don't reply to emails or texts asking for personal or tax information. Be cautious to whom you provide personally identifying information (PII).
- Don't click on unknown links or links from unsolicited messages. Type the organization's website address into your web browser.
- Don't open attachments from unsolicited messages as they may contain malware.
- Don't conduct financial business over public, guest, free, or insecure Wi-Fi networks.
- Don't necessarily trust "HTTPS" to mean a site is legitimate. There has been an increase in the use of HTTPS sites being used by phishers.
- Never discard documents in the trash that have critical information, such as personal or financial data. Shred all unneeded documents containing confidential information.
- Check 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.

For more information about tax scams, visit https://www.irs.gov/uac/tax-scams-consumer-alerts. If you suspect you have become a victim of tax fraud or identity theft, the IRS encourages you to visit https://www.identitytheft.gov/. This site provides a step-by-step recovery plan and assistance for taking action. 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. You can also call the IRS at 800-908-4490. ***Note:*** *Be sure to check out the* ***Stay Safe From Cybercrime During Tax Time Tip Sheet*** *attached to this newsletter.*

Ransomware Attacks Again!

Another NC local government has been affected by ransomware! Last year, a similar incident occurred in Mecklenburg County where a foreign-based hacker gained access to a government employee's log-in information and launched a ransomware attack. That incident compromised government systems and left many services offline for several weeks. This time, Davidson County has become the victim of a recent ransomware attack, after county systems were infected on Friday, February 16, 2018. The County's 911 director notified the County's Chief Information Officer (CIO) that suspicious activity was detected within their 911 system. County officials soon discovered they had been compromised by a ransomware called *SamSam*. According to county officials, system files were encrypted and unavailable for use, but no data was stolen. The hackers demanded an undisclosed amount of Bitcoin, a type of cyber currency, and gave the county seven days to pay the ransom. The investigation is still ongoing, but the suspected means of attack is phishing.

Ransomware has become the tool of choice for cybercriminals in recent years. According to Malwarebytes, between September 2015 and September 2017, the number of ransomware attacks detected increased by 1,989%. While many ransomware attacks use phishing emails or drive-by downloads to infect a system, ransomware like SamSam usually gains access to a victim's network by exploiting vulnerabilities in a system and then spreads to other connected systems. Incidents like the Mecklenburg and Davidson County attacks show that even though an organization may spend millions of dollars to secure its systems and data, one vulnerable system or one person clicking on a malicious link in an email can compromise the entire organization. So, what steps can be taken to minimize the risk of a ransomware attack?

- ***Be leery of unexpected messages and attachments:*** Don't open attachments or click links in emails you were not expecting, even if they appear to come from someone you know. It is safer to not click on links in an email message, but rather manually type the web address.
- ***Ask for confirmation:*** If a message seems suspicious and asks for a response, call the sender using a known phone number that did not originate from the suspicious email – like your personal address book or the "contact us" page on a legitimate website.
- ***Don't provide personal information when answering unsolicited calls/messages:*** Phishers try to trick employees into installing malware, or gain intelligence for attacks by claiming to be someone they trust. Be sure to report any suspicious calls or emails you may receive using your organization's documented reporting process.
- ***Use a reputable and up-to-date antivirus software and firewall:*** Maintaining a strong firewall and keeping your security software up to date are critical. It is important to use antivirus software from a reputable company because of all the fake software out there.
- ***Make sure all systems and software are up-to-date with relevant patches:*** Exploit kits hosted on compromised websites are commonly used to spread malware. Regular patching of vulnerable software is necessary to help prevent infection.
- ***Ensure regular backups are done AND they are protected:*** If you become a victim of ransomware, a good and recent backup may be the only way to safely recover your data.

For more information about ransomware and what you can do about it, visit the following: https://www.cisecurity.org/ransomware-facts-threats-and-countermeasures/

Don't forget the other **monthly newsletters** available to you! The following are the various cybersecurity newsletters the ESRMO distributes each month. We hope you find them beneficial.

- **SECURITYsense Newsletter:** A licensed newsletter for State employees that contains several articles involving current cybersecurity issues. **Note:** *You must have a Microsoft O365 account with access to the ESRMO external SharePoint site to access this resource*.

https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/SECURITYsense

- **Security Tips Newsletter:** A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's edition is on ***Spotting and Avoiding Olympic 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 ***Securing Your Mobile Devices.***

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

---

NISC National Information Sharing Consortium

The National Information Sharing Consortium (NISC) will host a webinar with NISC bronze sponsor, CA Technologies, to provide an overview of the secure FirstNet onramp solutions they are developing for State and Local applications and data. Absolute control over State and Local first responder systems and applications has always been a priority.

State and Local governments want to keep their applications running on their choice of infrastructure but also want interoperability with the anticipated FirstNet applications/ capabilities. This requires secure bridging/interoperability/access control functionality built to work with FirstNet. The goal is to create a secure FirstNet Interoperability "Onramp" for State and Local applications and their data, preconfigured to provide deep visibility into application traffic and load tested to ensure everything works when needed. This webinar will introduce CA Technologies and the company's solutions for ensuring the security, performance, interoperability and testing of first responder apps – assuring readiness for use via FirstNet.

Date/Time: Wednesday, March 14, 2018 @ 1-2 pm (ET)

Speakers:

- Sean McSpaden, Executive Director, National Information Sharing Consortium
- Mary Lou Prevost, Vice President, State and Local Government and Education Programs, CA Technologies
- Keith Athey, Senior Business Technical Architect, CA Technologies

To register for the webinar, click the following link:
https://register.gotowebinar.com/register/539971647730464515

Don't forget the following resources:

- Department of Information Technology (DIT) Site: https://it.nc.gov/
- Cybersecurity and Risk Management Site: http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management
- Cybersecurity Awareness Page: https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness
- State of NC Cybersecurity Situation Report Site: https://it.nc.gov/cybersecurity-situation-report

Did you know that The SANS Institute also provides *free* awareness **videos** and **webcasts**? The SANS Video of the Month may be accessed at https://securingthehuman.sans.org/resources/votm.

Also, The SANS Institute offers free webcasts on a variety of topics that may be accessed at https://www.sans.org/webcasts/upcoming.

Upcoming SANS Webcasts:

2/27/2018 – *Why Insider Actions Matter: SANS Review of LogRhythm CloudAI for User and Entity Behavior Analytics*

3/1/2018 – *52% of Companies Sacrifice Cybersecurity for Speed*

3/20/2018 – *Data on the Dark Web: finding your corporate data before the criminals do*

3/29/2018 – *Being Offensive in the Workplace*

Access to these webcasts as well as a list of many others may be found via the link above!

FEMA

EMI e-Forums are 1-hour, moderated, webinar discussion forums that provide an opportunity for the Emergency Management Institute (EMI) and the emergency management community to discuss matters of interest on national preparedness training. These exchange of ideas and best practices are free of charge and available to anyone who wishes to participate. The forums are scheduled on **Wednesdays in March** from 3:00 – 4:00 p.m. EST.

- **3/7** – Applying Instructional Design Strategies and Behavior Theory to Household Disaster Preparedness Training
- **3/14** – VOADS and Government: Shared Training Resources
- **3/21** – Incorporating Reusable Learning Objects (RLOs) in Training: How to Use from an Instructional Systems Designer
- **3/28** – Homeland Security Exercise and Evaluation Program (HSEEP): Beyond the Templates

Login link: https://fema.connectsolutions.com/emieforums

Conference call-in: 800-320-4330, PIN 107622

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 in order 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.

STAY SAFE FROM CYBERCRIME DURING *TAX TIME*

Everyone's favorite time of year – tax season – is creeping up on the calendar. Tuesday, April 17, may feel eons away, but the filing deadline will be here before you know it. Tax season is primetime for online scams. According to the Federal Trade Commission (FTC), tax-related identity theft – when a criminal uses someone else's Social Security number along with other personal data to file an income tax return (and reap any refunds) – is the most common type of identity theft. In fact, a 2017 Identity Fraud Study by Javelin Strategy & Research revealed that nearly one in three consumers notified that their data has been breached become victims of identity fraud. With the recent Equifax cyberattack still fresh in our minds, more than 145 million Americans' names, addresses, birthdates, Social Security numbers and other sensitive information may be at risk. Cybercriminals are crafty and continuously looking for ways to steal your personal information. The Internal Revenue Service (IRS) indicates that phishing schemes continue to lead its "dirty dozen" list of 2017 tax scams. So what is the average American to do? The National Cyber Security Alliance (NCSA) and the Identity Theft Resource Center (ITRC) have once again joined forces to help consumers keep safe during tax season with tips for identifying cyber scams, actionable online safety steps and what to do if you fall victim to tax identity theft.

SCAMS TARGETING TAXPAYERS

The IRS has a seen a surge in cybercriminal swindles directed at consumers. If you protect yourself against these unscrupulous schemes, your identity and tax return will be safer and more secure.

IRS-IMPERSONATION PHONE SCAMS

Callers claiming to be IRS employees – using fake names and phony IRS ID numbers – may ring you and insist that you owe money and it must be paid as soon as possible through a gift card or wire service. If the call is not picked up, the scammers often leave an emergency callback request message. The real IRS will not call you and demand immediate payment; in general, it will mail you a bill if you owe money.

MARKED INCREASE IN PHISHING, EMAIL AND MALWARE SCHEMES

Cybercriminals will try to get you to do something so they can steal your personal information. Watch out for unsolicited emails, text messages, social media posts or fake websites that may prompt you to click on a link or to share valuable personal and financial information. Armed with this information, online thieves can pilfer funds and/or commit identity theft. And unfamiliar links or attachments can contain malware – viruses, spyware and other unwanted software that gets installed on your computer or mobile device without your consent – which can infect your computer files if opened.

STAY SAFE FROM CYBERCRIME DURING *TAX TIME*

NATIONAL CYBERSECURITY ALLIANCE

ITRC IDENTITY THEFT RESOURCE CENTER

FRAUDULENT TAX RETURNS

The FTC strongly recommends trying to file your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If the file is yours and it's in early, it becomes impossible for a fraudster to submit another return with your personal information. It's also important to always use smart practices with your personal information. Remember to only share your Social Security number when it's absolutely necessary. Check your credit report regularly for shady activity, and never throw papers with critical information – like your Social Security number or bank account information – in the trash. It's best to shred all paper containing personal data.

TAX PREPARER FRAUD

The overwhelming majority of tax preparers provide honest services, but some unsavory individuals may target unsuspecting taxpayers and the result can be refund fraud and/or identity theft. The IRS reminds anyone filing a tax return that their preparer must sign it with their IRS preparer identification number.

TAKE ACTION AND STAY CYBER SAFE WITH TAX TIPS

NCSA has some easy-to-use STOP. THINK. CONNECT.™ tips to help protect against fraudster tricks:

KEEP ALL MACHINES CLEAN

Having updated software on all devices that connect to the internet is critical. This includes security software, web browsers and operating systems for PCs and your mobile devices. Having current software is a strong defense against viruses and malware that can steal login credentials or use your computer to generate spam.

LOCK DOWN YOUR LOGIN

Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.

MAKE BETTER PASSWORDS

If your passwords are too short or easy to guess, it's like giving a cyber thief your banking PIN. Longer passwords and those that combine capital and lowercase letters with numbers and symbols provide better protection.

GET SAVVY ABOUT WI-FI HOTSPOTS

Public wireless networks are not secure. Cybercriminals can potentially intercept internet connections while you are filing highly personal information on public WiFi.

WHEN IN DOUBT, THROW IT OUT

Links in email are often the way bad guys get access to your personal information. If it looks weird, even if you know the source, it's best to delete.

THINK BEFORE YOU ACT

Be leery of communications that implore you to act immediately – especially if you are told you owe money to the IRS and it must be paid promptly.

FILE YOUR TAX FORMS ON SECURE HTTPS SITES ONLY.

ASK IF YOUR TAX PREPARATION SERVICE HAS CHECKED FOR MALWARE ISSUES.

STAY SAFE FROM CYBERCRIME DURING *TAX TIME*

NATIONAL CYBERSECURITY ALLIANCE

ITRC IDENTITY THEFT RESOURCE CENTER

WHAT YOU NEED TO KNOW ABOUT TAX IDENTITY THEFT

According to ITRC, the most important step you can do is file early and get your tax refund before thieves do. Follow these steps to get help as a victim of tax identity theft:

- **If you suspect identity theft**: If you think you have tax issues related to identity theft, call the IRS Identity Protection Specialized Unit (IPSU) at 1-800-908-4490.
- **File an ID theft affidavit:** You can document the identity theft by submitting a police report and the IRS ID Theft Affidavit (Form 14039)
- **Contact your state tax organization:** Your state taxes may be affected as well.
- **Document your case:** Download the **free ID Theft Help app** from ITRC to track your case as you go through the resolution process.
- **Call the ITRC:** You can receive no-cost assistance from a victim advisor by calling 1-888-400-5530.

REMINDERS FROM NCSA AND ITRC

"Cybercriminals love tax season. The enormous amounts of valuable personal and financial information that are shared online during this timeframe make it a haven for hackers. Since most Americans are filing their taxes, deadlines are looming and the cyber thugs are doing everything they can to take full advantage of the opportunity," said Russ Schrader, the National Cyber Security Alliance's executive director. "Hackers are masters of social engineering, so when there is increased potential for having your most personal data exposed, it's critically important to take steps to use the internet safely and more securely. Remember that Personal Information Is Like Money. Value It. Protect It. Practicing good cybersecurity – when preparing your tax returns and all year round – empowers internet users to reap the benefits of connectivity with greater confidence."

"Identity thieves continue their tax-time fraud exploits on two fronts: tax identity fraud and IRS imposter scams," said Eva Velasquez, president & CEO of the Identity Theft Resource Center. "That means every stakeholder needs to increase his/her vigilance in minimizing risk. In our current climate of ubiquitous data breaches, consumers can feel powerless; however, they do play a vital role in the risk equation. By making informed choices when sharing data and identity credentials, filing tax returns as early as possible and verifying they are actually speaking to the IRS, a consumer can thwart identity thieves."

RESOURCES TO HELP YOU STAY SAFE THIS TAX SEASON

Here are a few resources that can help you protect your identity and be safer and more secure online this tax season – and year-round:

- STOP. THINK. CONNECT.™ Tips and Advice
- Identity Theft Resource Center
- The Federal Trade Commission's IdentityTheft.gov
- The Internal Revenue Service's Tax Scams and Consumer Alerts
- The U.S. Department of Homeland Security's STOP. THINK. CONNECT.™ Identity Theft and Internet Scams Tip Card

STAYSAFEONLINE.ORG

STAYSAFEONLINE STAYSAFEONLINE

IDTHEFTCENTER.ORG

ITRCSD ITRCSD