Monthly Cybersecurity Newsletter

January 2020
Issue

Enterprise Security and Risk Management Office (ESRMO)

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

Stay Safe from Cybercrime During Tax Time

Cybercriminals love tax season.

The enormous amounts of valuable personal and financial information shared online during this time of year make it a haven for thieves – and they are doing everything they can to take full advantage of the opportunity tax season brings them. They are masters at social engineering. So, during this time of increased potential for having your personal information exposed, it's critically important to take steps to use the internet safely.

Remember that your personal information is like money. Identity thieves continue their tax-time fraud exploits on two fronts: tax identity fraud and IRS imposter scams. By making informed choices when sharing your personal information, by filing your tax returns as early as possible and by verifying that you're speaking to the IRS, you can thwart these identity thieves.

Here are four ways cybercriminals try to take advantage of taxpayers during tax season:

- **IRS impersonation scams:** Callers claiming to be IRS employees might call and insist that you owe money and that it must be paid as soon as possible via gift card or wire service. If the call isn't picked up, they leave an emergency callback message. The IRS will never call you to demand immediate payment. They will mail you a bill if you owe money.
- **Marked increase in phishing, email and malware schemes:** Watch for unsolicited emails, texts, social media posts or fake websites that might prompt you to click a link or share personal and financial information. Cybercriminals can use such information to steal your money and/or your identity. Unfamiliar links or attachments can also contain viruses, spyware or other malware that get installed on your computer or mobile device without your knowledge.
- **Fraudulent tax returns:** File your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If you file early, it becomes impossible for a fraudster to submit another return with your personal information.
- **Tax preparer fraud:** The overwhelming majority of tax preparers provide honest services, but some unsavory individuals might 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.

STAY SAFE DURING 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

Avoiding Social Engineering and Phishing Attacks

Social engineering is when an attacker uses human interaction (social skills) to obtain information about an organization or its computer systems.

The attacker might seem unassuming and respectable – possibly claiming to be a new employee, a repair person or a researcher. By asking questions, they might be able to piece together enough information to infiltrate an organization's network.

If the attacker is not able to gather enough information from one source, they might contact another source within the same organization and rely on the information from the first source to add to their credibility.

Three forms of social engineering are phishing (email), vishing (telephone) and smishing (text messages). Here are five common indicators of phishing attempts:

- **Suspicious sender's address:** The sender's address might imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.

- **Generic greetings and signature:** Both a generic greeting – such as "Dear Valued Customer" or "Sir/Ma'am"– and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide its contact information.

- **Spoofed hyperlinks:** If you hover your cursor over any links in the body of the email and the links do not match the text that appears when hovering over them, the link might be spoofed. Malicious websites can look identical to a legitimate site, but the URL might use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals might use a URL shortening service to hide the true destination of the link.

- **Spelling and layout:** Poor grammar and sentence structure, misspellings and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify and proofread customer correspondence.

- **Suspicious attachments:** An unsolicited email requesting that a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal might use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

Here are eight ways to avoid becoming a victim of social engineering attacks:

- Be suspicious of unsolicited phone calls, visits or emails from individuals asking about employees or other internal information. If an individual you don't know claims to be from a legitimate organization, try to verify their identity directly with the company.
- Do not provide personal information or information about your organization unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in emails.
- Do not send sensitive information over the internet before checking that the website is secured with a padlock icon in the URL or that it has a valid certificate.
- Pay attention to the URL of a website. Do not click on the link in an email, but rather use a URL that you know is valid.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request. Instead, check previous statements for contact information.
- Install and maintain anti-virus software, firewalls and email filters to reduce the risk of malicious/suspicious traffic.
- Take advantage of anti-phishing features offered by your email client and web browser.

Security Awareness Tip of the Month

What is malware?

Malware is software – a computer program – used to perform malicious actions. In fact, the term malware is a combination of the words malicious and software. Cybercriminals place malware on your computers or devices to gain control over them or to gain access to what they contain.

Malware is most often installed unwittingly by the end user by means of clever social engineering techniques. Once installed, these attackers can use malware to spy on your online activities, steal your passwords and files or use your system to attack others.

CYBERSECURITY NEWSLETTERS

Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4.
***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: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month, the newsletter covers ***New year, New You… Same W-2 Tax Scam***.

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Digital Inheritance.***

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

Feb. 5: Your Password Doesn't Matter Webinar

Feb. 6: Implementer's Guide to Deception Technologies Webinar

Feb. 19: Real-World Implementation of Deception Technologies Webinar

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. You are also encouraged to review Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember…Stop. Think. Connect.*