Volume 15, Issue 1 • Jan. 2020 | **Monthly Security Tips Newsletter**

WV Executive Branch
Privacy Tip

New Year, New You… Same W-2 Tax Scams

Tax season is in full swing, which means criminals will go to great lengths to separate you from your money, your identity, or anything of value that is within their reach. They may offer seemingly legitimate "tax services" that are actually designed to steal your identity and your tax refund. Often times, criminals will lure you in with an offer of larger write-offs or refunds. Such scams might include fake websites and tax forms that look like they belong to the Internal Revenue Service (IRS) in order to trick you into providing your personal information.

Due to the rise in data breaches, you should always take steps to minimize your risk of identity theft and other online-related crimes; this is especially important this time of the year. Below are some warning signs to look for and basic precautions you can take to minimize risk and avoid becoming the next victim!

Warning Signs of an Online Tax Scam

- An email or link requesting personal and/or financial information, such as your name, social security number, bank or credit card account numbers, or any additional security-related information.
- Emails containing various forms of threats or consequences if no response is received, such as additional taxes or blocking access to your funds.
- Emails from the IRS or federal agencies. The IRS will not contact you via email.
- Emails containing exciting offers, tax refunds, incorrect spelling, grammar, or odd phrasing throughout.
- Emails discussing "changes to tax laws." These email scams typically include a downloadable document (usually in PDF format) that purports to explain the new tax laws. However, unbeknownst to many, these downloads are almost always populated with malware that, once downloaded, will infect your computer.

How to Avoid Being the Victim

- **Never Send Sensitive Information in an Email:** Information sent through email can be intercepted by criminals. Make sure to consistently check your financial account statements and your credit report for any signs of unauthorized activity.
- **Secure Your Computer:** Ensure your computer has the latest security updates installed. Check that your anti-virus and anti-spyware software are running properly and receiving automatic updates from the vendor. If you haven't already done so, install and enable a firewall.
- **Carefully Select the Sites You Visit:** Safely searching for tax forms, advice on deductibles, tax preparers, and other similar topics requires great caution. NEVER visit a site by clicking on a link sent in an email, found on someone's blog, or in an advertisement. The websites you land on might look like legitimate sites, but can also be very well-crafted fakes.

- **Be Wise with Wi-Fi:** Wi-Fi hotspots are intended to provide convenient access to the internet, however, this convenience can come at a cost. Public Wi-Fi is not secure and is susceptible to eavesdropping by hackers, therefore, never never use public Wi-Fi to file your taxes!
- **Look for Clear Signs:** Common scams will tout tax rebates, offer great deals on tax preparation, or offer a free tax calculator tool. If you did not solicit the information, it's likely a scam.
- **Be on the Watch for Fake IRS Scams:** The IRS will not contact you via email, text messaging, or your social network, nor does it advertise on websites. Additionally, if an email appears to be from your employer or bank claiming there is an issue that requires you to verify personal information, this is most likely a scam as well. Don't respond to these types of emails; always contact the entity directly.
- **Always Utilize Strong Passwords:** Cybercriminals have developed programs that automate the ability to guess your passwords. To best protect yourself, make your passwords difficult to guess. Passwords should have a minimum of nine characters and include uppercase and lowercase letters, numbers, and symbols.

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 (with headers or 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.

For More Information

- IRS | Taxpayer Guide to Identity Theft
- IRS | Report Phishing
- IRS Dirty Dozen

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.