From the desk of
Michael Aliperti
MS-ISAC Chair

Don't be Frivolous With Your Stimulus

Seasonal Scams Ensue, Protect Your W-2

It seems like it's been much longer than one year ago since we last did our taxes, but somehow, it's here again; Tax season. Let's start out by acknowledging that this past year, fiscally, is fundamentally different from other tax years before it. The introduction of Stimulus payments from the government in the past year has added a new dimension to our taxes, and a potential increase of vulnerability to hackers and cyber criminals alike.

This is a period of time where extra vigilance and caution is needed while online and conducting business, especially avoiding any kind of online activity that could jeopardize your identity and finances. There are some important best practices and red flags to keep in mind while navigating through this season, and hopefully you'll feel a little bit more secure with the knowledge that you haven't fallen victim to a cyber scheme!

Scams to look out for

- An email, link, or phone call requesting personal and/or financial information, such as your name, social security number, bank or credit card account numbers, or any security-related information.
- Receipt of a notice that states your IRS account has been accessed or disabled when you haven't accessed the account.
- Emails advertising bigger tax refunds, or that have incorrect spelling, grammar, or odd phrasing throughout.
- Emails that tell a story and entice you to open a link or attachment. Sometimes they will say they've noticed suspicious activity, claim there is a problem with your account, or want you to click on a link to make a payment. These links often contain malware that is used to infect your computer and retrieve your personal information.

Stimulus-specific scams

- **Scammers have been mailing out fraudulent checks that appear to be sent from the government,** and will request that money be sent back due to an "over-payment." Always call your bank to verify a check is legitimate, and if you receive a request to return a portion of a check, report this immediately to your bank.
- **Robo-call check scams are commonly reported.** The caller will be asking for personal and/or financial information and try to convince you that this information is necessary in order for the check to be deposited. In reality, the government already has your information on file from when you completed your taxes. You will either get your stimulus check and tax refund in the mail or they will be directly deposited to your account.
- **Carefully Select the Sites You Visit:** Do not visit a site that doesn't end in ".gov". No non-governmental website is distributing stimulus checks.

How to avoid being a victim

- **Never Send Sensitive Information in an Email:** If there is any doubt that communication is coming from a suspicious source, don't reply to any email requesting personal information.
- **Keep Up your Cyber Hygiene:** Keep up to date with recent data breaches. 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. Change your passwords frequently.
- **Carefully Select the Sites You Visit:** Do not click on links sent to you via email from a site claiming to give tax preparation advice or tax forms as there are many fake forms on scam sites that look authentic.
- **Never Use Public Wi-Fi to File Your Taxes!**
- **Only Use a Bona-fide Preparer:** If you choose to use a preparer to do your taxes, make sure they can provide their Tax Preparer Identification Number – you can use this number to look them up on the IRS website to confirm they are legitimate, as only professionals can hold this identification.
- **Be Aware of IRS Typical Practices:** The IRS will not contact you via email, text messaging, or your social network, nor does it advertise on websites. Starting in 2021, the IRS has created IP PINS available for all taxpayers. These PINS provide the IRS additional verification and security at the time of filing. You can log on to get an IP PIN tool offered by the IRS at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin/.
- **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.

For more information

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

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

1.