fraudsters continue to use the pandemic as a way of tricking people into sharing sensitive personal information by email, text message and online. Identity thieves can use that ...

Nov. 23, 2021

With the holidays just around the corner and the 2022 tax season getting closer, scammers are ramping up their activities too. As such, Americans are being urged to take extra care to protect sensitive financial information.

The Security Summit partners, a coalition of the IRS, state tax agencies, tax

financial information to help slip past common defenses. That has made tax professionals – who hold valuable tax information for their clients – a tempting target for scam artists.

"The nation's tax community has successfully joined forces to protect taxpayers through the Security Summit effort, but we need help in this continuing battle," said IRS Commissioner Chuck Rettig. "Taxpayers and tax professionals are the first line of defense against scammers looking for refunds. We are entering a sensitive holiday and tax period, and we urge people to protect their personal information – and avoid problems at tax time."

The IRS and Summit partners continue to see constantly evolving threats and scams. They can mimic IRS and others in the tax community with fake emails, texts and online scams. These schemes can lurk underneath COVID-related messages, stimulus payments or tax refunds. And they can frequently use recent tragedies or charitable groups to coax people into sharing sensitive financial data.

To help combat this, the Summit partner's National Tax Security Awareness Week will feature a week-long series of educational materials to help protect individuals, businesses and tax pros from identity theft. The effort will include special informational graphics and a social media effort on Twitter and Instagram with @IRSnews and #TaxSecurity.

A special emphasis for this year will be focusing tax security awareness on younger and older Americans. Even if someone doesn't file a tax return, their online interactions can lead to scam artists obtaining sensitive information and using it to try obtaining a refund.

As part of the larger effort, the IRS and Security Summit partners are sharing YouTube videos on security steps for taxpayers. The videos can be viewed or

downloaded at Easy Steps to Protect Your Computer and Phone and Security

- Use security software for computers and mobile phones – and keep it updated.
- Avoid phishing scams, especially related to tax refunds and COVID-19, Economic Impact Payments and other tax law changes.
- Use strong and unique passwords for all accounts.
- Use multi-factor authentication whenever possible.
- Shop only secure websites; look for the "https" in web addresses and the padlock icon; avoid shopping on unsecured and public Wi-Fi in places like coffee shops, malls or restaurants.

Day 2 – Giving Tuesday: Beware of scammers using fake charities

The IRS and the Security Summit partners warn people to avoid getting scammed when donating to charities. The agency provides the following tips:

- Individuals should never let any caller pressure them into giving a donation without allowing time for them to do some research.
- Confirm the charity is real by asking for its exact name, website and mailing address and confirming it later.
- Be careful about how a donation is made. After researching the charity, pay by credit card or check and not by gift card or wiring money.

Day 3 – Get an Identity Protection PIN

Taxpayers who can verify their identities online may opt into the IRS IP PIN program – a major expansion of the program from previous years. This is another tool taxpayers can use to protect themselves – and their tax refund. Here's what taxpayers need to know:

- The Identity Protection PIN or IP PIN is a six-digit code known only to the individual and the IRS. It provides another layer of protection for taxpayers' Social

Security numbers on tax returns.

- Deploy basic security measures.
- Use multi-factor authentication to protect tax software accounts.
- Create a Virtual Private Network if working remotely.
- Create a written data security plan as required by federal law.
- Know about phishing and phone scams, especially related to Electronic Filing Identification Numbers (EFINs), COVID-19 related tax-law changes including Economic Impact Payments.
- Create data security and data theft recovery plans.

Day 4 – Use digital signatures to submit IRS forms and check account details on secure portal

The IRS began accepting digital signatures on a variety of forms this past year. Additionally, the agency made improvements to its online accounts platform to help both tax pros and individuals.

- Tax pros may go to the new Tax Pro Account on IRS.gov to digitally initiate Power of Attorney and Tax Information Authorization requests.
- Taxpayers have digital control over who can represent them or see their account information on the Online Account portal.
- The IRS now accepts a wide array of digital signatures on a number of forms that cannot be electronically filed.

Day 5 – Businesses should implement safeguards; watch out for tax-related scams

Most cyber attacks are aimed at small businesses with fewer than 100 employees. Here are some details from this segment:

- Learn about best security practices for small businesses.
- IRS continues protective masking of sensitive information on business transcripts.

- A Business Identity Theft Affidavit – Form 14039-B – is available for all businesses

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.