Security Summit partners announce National Tax Security Awareness Week dates; urge increased security measures as fraudsters exploit COVID-19 concerns

WASHINGTON − The Internal Revenue Service, state tax agencies and the nation's tax industry today announced that the 5th Annual National Tax Security Awareness Week will take place between Nov. 30 and Dec. 4.

This year, there's a heightened need for security as fraudsters seek to use the COVID-19 to scam taxpayers and tax preparers. New protections being offered by Security Summit partners in January can help protect people against tax-related identity theft.

"As the holiday season and tax season approach, everyone should remember to take basic steps to protect themselves," said IRS Commissioner Chuck Rettig. "With more taxpayers and tax preparers working remotely, identity thieves are trying to use COVID-19 to scare and scam people out of their identities or money. All of us must be on guard and use the strongest security measures we can. The goal of National Tax Security Awareness Week is to remind people about important steps they can take to protect themselves and their tax information."

The IRS warned taxpayers to remain vigilant due to constantly evolving threats and scams from fraudsters. There are thousands of variations of COVID-related scams, including many related to the economic stimulus payment by the IRS.

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.

As part of the 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 Avoid Phishing Emails.

Employers also can share Publication 4524, Security Awareness for Taxpayers, with their employees and customers while tax professionals can share with clients.

The National Tax Security Awareness Week features basic security guidance for those most at-risk: individual taxpayers, business taxpayers and tax professionals. Highlights include:

Day 1: Cyber Monday: Protect personal and financial information online
The IRS and the Security Summit partners remind people to take these basic steps:

1. Use security software for computers and mobile phones – and keep it updated.
2. Avoid phishing scams, especially related to COVID-19 or Economic Impact Payments.
3. Use strong and unique passwords for all accounts.
4. Use multi-factor authentication whenever possible.
5. 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 shopping malls.

Day 2: Use multi-factor authentication
Remember to use multi-factor authentication options being offered by tax software providers:

1. All tax software providers are offering multi-factor authentication options on products for both taxpayers and tax professionals.
2. Multi-factor authentication protects online accounts by requiring a second verification code in addition to your credentials (username and password.) This second feature may be a code sent to your mobile phone, for example.
3. Multi-factor authentication provides a critical layer of protection for your online accounts.

Day 3 – Get an Identity Protection PIN
Starting in January, taxpayers who can verify their identities may now opt into the IRS IP PIN program. Here's what you need to know:

1. The Identity Protection PIN or IP PIN is a six-digit code known only to you and the IRS. It provides another layer of protection for taxpayers' Social Security numbers on tax returns.
2. Use the Get An Identity Protection PIN (IP PIN) tool at IRS.gov/IPPIN to see if the IP PIN is right for you and to immediately get an IP PIN.
3. Never share your IP PIN with anyone but your trusted tax provider.

Day 4 – Businesses at risk for identity theft
Most cyberattacks are aimed at small businesses with fewer than 100 employees. Here's are some details:

1. Learn about best security practices for small businesses.
2. IRS protective masking of sensitive information on business transcripts starts December 13.
3. A Business Identity Theft Affidavit – Form 14039-B – is now available for all businesses to report theft to the IRS.
4. Beware of various scams, especially the W-2 scam that attempts to steal employee income information.
5. Check out the "Business" section on IRS' Identity Theft Central at IRS.gov/identify theft.

Day 5 – Tax professionals should review their safeguards
The IRS and the Summit partners urge tax pros to review the "Taxes-Security-Together" Checklist, including:

1. Deploy basic security measures.
2. Use multi-factor authentication to protect tax software accounts.
3. Create a Virtual Private Network if working remotely.
4. Create a written data security plan as required by law.
5. Know about phishing and phone scams, especially related to fake clients, COVID-19 and the Economic Impact Payments.
6. Create data security and data theft recovery plans.