pandemic, nationwide teleworking practices and other events as predatory ...

Isaac M. O'Bannon • Jul. 15, 2022

As the battle continues against tax-related identity theft, the IRS, state tax agencies and the tax industry renewed their call for tax professionals to be on guard against new and ongoing threats involving their systems and taxpayer data.

This effort begins next week with the Security Summit's annual summer campaign focused on tax professionals and taking fundamental steps to stop data theft from

their offices. This is the seventh year that the Security Summit partners – the IRS,

to protect the federal and state tax systems from identity thieves," said IRS Commissioner Chuck Rettig. "As we've increased our defenses, cyberthieves increasingly turn to tax professionals, especially smaller operations, to look for security vulnerabilities. This is a critical link in protecting sensitive taxpayer information. By taking some basic security steps, tax pros help protect against the relentless efforts of identity thieves."

This summer's effort focuses on a reminder for tax pros to focus on fundamentals and to watch out for emerging vulnerabilities being seen for those practitioners using cloud-based services for their practice.

Identity thieves were especially active this past year as they continued to use the pandemic, nationwide teleworking practices and other events as predatory tactics for a variety of scams.

Tax professionals are prime targets of criminal syndicates that are both tech- and tax-savvy and well-funded. These scammers either trick or hack their way into tax professionals' computer systems to access client data. Even when tax pros think they have client data stored in a secure cloud, lack of strong authentication can make this information vulnerable.

Thieves can use stolen data to file fraudulent tax returns that make it more difficult for the IRS and the states to detect because the fraudulent returns use real financial information. Other data thieves sell the basic tax preparer or taxpayer information on the web so other fraudsters can try filing fraudulent tax returns.

The Security Summit formed in 2015 to join the fight against identity theft. The Summit partners made great inroads against tax-related identity theft, dramatically reducing confirmed identity theft returns and saving billions in tax dollars.

During the next five weeks, the Security Summit partners will highlight a series of

from filing a fraudulent return in the taxpayer's name. Tax professionals cannot obtain an IP PIN for their clients. Clients must verify their identities to the IRS. The easiest way is at the Get an IP PIN tool on IRS.gov. The IRS Electronic Tax Administration Advisory Committee recently described the IP PIN as" the number one security tool currently available to taxpayers from the IRS. This tool is the key to making it more difficult for criminals to file false tax returns in the name of the taxpayer."

- **Avoid spear phishing scams.** One of the most successful tactics used by identity thieves against tax professionals is the spear phishing scam. Thieves take time to craft personalized emails to entice tax professionals to open a link embedded in the email or open an attachment. Tax pros have been especially vulnerable to spear phishing scams from thieves posing as potential clients. Thieves might carry on an email conversation with their target for several days before sending the email containing a link or attachment. The link or attachment may secretly download software onto the tax pros' computers that will give thieves remote access to the tax professionals' systems.
- **Know the tell-tale signs of identity theft.** Many tax professionals who report data thefts to the IRS also say that they were unaware of the signs that a theft had occurred. There are many signs that tax pros should watch for. These include multiple clients suddenly receiving IRS letters requesting confirmation that they filed a tax return deemed suspicious. Tax professionals may see e-file acknowledgements for far more tax returns than they filed. Computer cursors may move seemingly on their own.
- **Create a security plan.** Not only is it a good practice, the IRS also reminds tax professionals that federal law, enforced by the Federal Trade Commission, requires paid tax return preparers to create and implement a data security plan. An information security plan protects the business and client information while also providing a blueprint for action in the event of a security breach. For many tax

professionals, knowing where to start when developing a written security plan

protect not only the tax professional, but their clients alike.

This summer series runs for five weeks and coincides with the annual IRS Nationwide Tax Forums, which are being held virtually beginning July 19. The forums feature three webinars focused on cyber- and information security that will be live streamed as follows:

- **Cybersecurity for Tax Professionals – Advanced Session**, presented by the American Coalition for Taxpayer Rights, July 21 at 2 p.m. ET.
- **Deeper Dive into Emerging Cyber Crimes and Crypto Tax Compliance**, July 26 at 11 a.m. ET.
- **Helping You and Your Clients Steer Clear of Fraud and Scams**, presented by the Treasury Inspector General for Tax Administration, August 2 at 11 a.m. ET.

Digital Currency • Taxes