CPA
Practice Advisor

Aug. 10, 2021

The Internal Revenue Service says that tax pros need to watch out for phishing scams that use various pandemic-related themes to steal client data.

The Security Summit partners continue to see instances where tax professionals, especially those who engage in remote transactions, have been vulnerable this year to identity thieves posing as potential clients. The criminals then trick practitioners into opening email links or attachments that infect computer systems.

Avoiding phishing emails is the fourth in a five-part series sponsored by the IRS, state tax agencies and the nation's tax community – working together as the Security Summit – highlighting critical steps tax professionals can take to protect client data. This year's theme "Boost Security Immunity: Fight Against Identity Theft," is an

effort to urge tax professionals to work to strengthen their systems and protect client

receiving the message into disclosing personal information such as passwords, bank account numbers, credit card numbers or Social Security numbers. Tax pros are a common target.

Scams may differ in themes, but they generally have two traits:

- They appear to come from a known or trusted source, such as a colleague, bank, credit card company, cloud storage provider, tax software provider or even the IRS.
- They tell a story, often with an urgent tone, to trick the receiver into opening a link or attachment.

A specific kind of phishing email is called spear phishing. Rather than the scattershot nature of general phishing emails, scammers take time to identify their victim and craft a more enticing phishing email known as a lure. Scammers often use spear phishing to target tax professionals.

In a reoccurring and very successful scam this year, criminals posed as potential clients, exchanging several emails with tax professionals before following up with an attachment that they claimed was their tax information. This scam was popular as many tax professionals worked remotely and communicated with clients over email versus in-person or over the telephone because of COVID.

Once the tax pro clicks on the URL and/or opens the attachment, malware secretly downloads onto their computers, giving thieves access to passwords to client accounts or remote access to the computers themselves.

Thieves then use this malware known as a remote access trojan (RAT) to take over the tax professional's office computer systems, identify pending tax returns, complete them and e-file them, changing only the bank account information to steal the refund.

In recent months, international criminals have used a ransomware attack to shut

accounts even if passwords were inadvertently disclosed. Keeping anti-virus software automatically updated helps prevent scams that target software vulnerabilities. Using drive encryption and regularly backing up files helps stop theft and ransomware attacks.

For tax professionals, securing their network to protect taxpayer data is their responsibility as a tax preparer.

To help tax professionals guard against phishing scams and better protect taxpayer information, the IRS recently updated Publication 4557, Safeguarding Taxpayer Data. The July 2021 version contains some of the latest suggestions such as using the multi-factor authentication option offered by tax software products and helping clients get an Identity Protection Pin.