ADV 2021-31
SECURITY SUMMIT

ADVISORY FOR TAX PROFESSIONALS
AUGUST 19, 2021

Tax professionals warned about evolving email scams

Identity thieves pose online as potential clients, Security Summit says

PROVIDENCE -- The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit warn tax professionals to beware of evolving phishing scams that use various pandemic-related themes to steal client data.

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

"Identity thieves have been relentless in exploiting the pandemic and the resulting economic pain to trick taxpayers and tax professionals to disclose sensitive information," said IRS Commissioner Chuck Rettig. "Fighting back against phishing scams requires constant vigilance, and we urge tax pros to take some basic steps to help protect their clients and themselves," he said.

Phishing emails or SMS/texts (known as "smishing") attempt to trick the person receiving the message into disclosing personal information such as passwords, bank account numbers, credit card numbers, or Social Security numbers. Tax professionals are a common target, said Rhode Island Tax Administrator Neena Savage.

Two main traits

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. Instead of using the scattershot nature of general phishing emails, criminals 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 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 because, due to the coronavirus (COVID-19) pandemic,

many tax professionals worked remotely and communicated with clients over email versus in-person or on the telephone.

Once the tax professional 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.

Ransomware attacks

In recent months, international criminals have used a ransomware attack to shut down a variety of companies. Criminals use similar, smaller-scale tactics against tax professionals. When the unsuspecting tax professional opens a link or attachment, malware attacks the tax professional's computer system to encrypt files and hold the data for ransom.

These scams highlight the importance of the basic security steps recommended by the Security Summit to protect data.

For example, using the two-factor or the multi-factor authentication option offered by tax preparation providers or storage providers would protect client 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 its Publication 4557 ("Safeguarding Taxpayer Data"). The new 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. To view the latest version: https://www.irs.gov/pub/irs-pdf/p4557.pdf

About this announcement

The Security Summit partners are conducting the 2021 "Protect Your Clients; Protect Yourself" summer campaign aimed at tax professionals. This year's theme is "Boost Security Immunity: Fighting Against Identity Theft". It's intended to urge tax professionals to step up their efforts to protect client data amid the pandemic and its aftermath. For more information: https://www.irs.gov/newsroom/security-summit.

The Rhode Island Division of Taxation is open to the public from 8:30 a.m. to 3:30 p.m. business days. To learn more, see the agency's website: www.tax.ri.gov.