IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Security Summit warns tax pros of evolving email and cloud-based schemes to steal taxpayer data

IR-2022-143, July 26, 2022

WASHINGTON – As part of a special Security Summit series, the Internal Revenue Service, state tax agencies and nation's tax industry warn tax professionals to beware of evolving scams designed to steal client data.

The Security Summit partners continue to see instances where tax professionals have been vulnerable to identity theft phishing emails that pose as potential clients. The criminals then trick practitioners into opening email links or attachments that infect computer systems with the potential to steal client information.

The Summit also warns tax professionals using cloud-based systems to store and prepare tax returns and information to make sure they use multi-factor authentication in light of recent attacks. Specifically, the Summit partners urge people using cloud-based platforms to use multi-factor options like phone, text or tokens. This can avoid potential vulnerabilities with authentication done just through email, which is easier for identity thieves to access.

Avoiding these schemes is the second in a five-part series from the IRS, state tax agencies and the nation's tax community – working together as the Security Summit that highlight critical steps tax professionals can take to protect client data. The focus of the Security Summit series – part of the Protect Your Clients, Protect Yourself campaign – is to urge tax professionals to work to strengthen their systems and protect client data.

"Identity theft scammers continually try new schemes to steal client personal and financial information from tax professionals. We continue to see a barrage of emails aimed at tax professionals trying to trick them into providing valuable access to identity thieves," said IRS Commissioner Chuck Rettig. "And we continue to urge people to use multi-factor authentication, including those using cloud-based services. Constant vigilance is necessary, not just during tax season but year-round. We urge tax pros, both large operations and smaller ones, to consider these invaluable recommendations to help protect their clients and themselves."

Phishing emails or SMS/texts (known as "smishing") attempt to trick the recipient 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 and other government agencies.
- They create a false narrative, 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, 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 gained energy as many tax professionals worked remotely and communicated with clients over email versus in-person or over the telephone because of the pandemic.

Once the tax pro clicks on the embedded 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 the past, criminals have used ransomware attacks to shut down a variety of companies. Criminals can use similar, smaller scale tactics against tax pros. When the unsuspecting tax professional opens a link or attachment, malware attacks the tax pro's computer system to encrypt files and the thieves hold the data for ransom.

Another emerging scheme the IRS has seen involves weak security from tax professionals using cloud-based systems to store client data. While many cloud-based systems are secure, tax professionals using these should ensure they're using strong multi-factor authentication on these to avoid thieves accessing their sensitive information.

The IRS has observed multiple instances – frequently involving smaller tax professionals or businesses – where individual accounts on cloud-based platforms have been compromised. Identity thieves' access these and then use existing data from taxpayer returns to file new tax returns seeking refunds, frequently by mail.

These cloud-based accounts are more vulnerable when tax pros do not use strong multi-factor authentication to validate who is using the platform. Summit partners urge using authentication methods besides email, which can be easier for thieves to access and allow entry into tax professional accounts. Using text, phone calls or tokens are safer options.

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

- Using the two-factor (2FA) or the multi-factor authentication (MFA) 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 also 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 Publication 4557, Safeguarding Taxpayer Data. This IRS publication 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.

Additional resources
In addition to reviewing IRS Publication 4557, Safeguarding Taxpayer Data, tax professionals can also

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

get help with security recommendations by reviewing Small Business Information Security: The Fundamentals by the National Institute of Standards and Technology. The IRS Identity Theft Central pages for tax pros, individuals and businesses have important details as well.

Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation of data theft information available on IRS.gov. Also, tax professionals should stay connected to the IRS through subscriptions to e-News for Tax Professionals and Social Media.

For more information, see IRS.gov.

-30-