CPA
Practice Advisor

increasing their attempts to use the pandemic and phishing scams to get access to sensitive client information.

Isaac M. O'Bannon • Dec. 03, 2021

Tax professionals face additional security risks from cybercriminals who are increasing their attempts to use the pandemic and phishing scams to get access to sensitive client information.

The IRS has urged tax pros to remain focused on security issues and ensure they

pandemic and other tricks to take advantage of tax pros and gain access to their data. We continue to urge tax preparers to remain aware of this changing threat. Taking important security steps can help avoid a security breach that can be devastating to them and their clients."

As the IRS and Security Summit partners took important steps to strengthen defenses against cybercriminals, identity thieves increasingly turned to tax professionals, targeting their offices and systems. Data thefts from tax professionals can provide valuable information to thieves trying to file fraudulent tax returns.

The Summit partners remind tax professionals to review their security measures. IRS Publication 4557, Safeguarding Taxpayer Data PDF, provides tax professionals with a starting point for basic steps to protect clients.

The Security Summit also created the "Taxes-Security-Together" Checklist to help tax professionals identify the basic steps they should take. As more tax preparers work from home or remote locations because of COVID-19, these measures are even more critical for securing tax data.

Basic protections – the "Security Six" measures

These easy steps can make a big difference, both for tax pros and taxpayers:

- Use anti-virus software and set it for automatic updates to keep systems secure. This includes all digital products, computers and mobile phones.
- Use firewalls. Firewalls help shield computers from outside attacks but cannot protect systems in cases where users accidentally download malware, for example, from phishing email scams.
- Use multi-factor authentication to protect all online accounts, especially tax products, cloud software providers, email providers and social media.

- Back up sensitive files, especially client data, to secure external sources, such as

for using multi-factor authentication. The Security Summit urges all tax professionals to use this option as the 2022 filing season approaches.

Practitioners can download to their mobile phones readily available authentication apps offered through Google Play or the Apple Store. These apps will generate a security code. Codes also may be sent to preparer’s email or text, but the IRS notes those are not as secure as the authentication apps. Search for “Authentication apps” in a search engine to learn more.

Use virtual private networks to protect remote sites

A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the company network. As teleworking or working from home continues during COVID-19, VPNs are critical to protecting and securing internet connections.

Failing to use VPNs can add risks to remote takeovers by cyberthieves, giving criminals access to the tax professional’s entire office network simply by accessing an employee’s remote internet.

Tax professionals should seek out cybersecurity experts whenever possible. Practitioners can also search for “Best VPNs” to find a legitimate vendor, or major technology sites often provide lists of top services. Remember, never click on a “pop-up” ad that’s marketing a security product. Those generally are scams.

Avoid phishing scams, including attempts to gain EFINs

Phishing emails generally have an urgent message, such as “your account password expired.” They direct users to an official-looking link or attachment. But the link may take users to a fake site made to appear like a trusted source, where it requests a username and password. Or, the attachment may contain malware, which secretly downloads software that tracks keystrokes and allows thieves to eventually steal all

> **== [Text of bogus email.] ==**
>
> > In order to help protect both you and your clients from unauthorized/fraudulent activities, the IRS requires that you verify all authorized e-file originators prior to transmitting returns through our system. That means we need your EFIN (e-file identification number) verification and Driver's license before you e-file.
> >
> > Please have a current PDF copy or image of your EFIN acceptance letter (5880C Letter dated within the last 12 months) or a copy of your IRS EFIN Application Summary, found at your e-Services account at IRS.gov, and Front and Back of Driver's License emailed in order to complete the verification process. Email: (fake email address)
> >
> > If your EFIN is not verified by our system, your ability to e-file will be disabled until you provide documentation showing your credentials are in good standing to e-file with the IRS.
> >
> > © 2021 EFILE. All rights reserved. Trademarks
> >
> > 2800 E. Commerce Center Place, Tucson, AZ 85706
>
> **== [End of bogus email text.] ==**

Tax professionals who received the scam should save the email as a file and then send it as an attachment to phishing@irs.gov. They also should notify the Treasury Inspector General for Tax Administration to report the IRS impersonation scam. Both TIGTA and the IRS Criminal Investigation division are aware of the scam.

Like all phishing email scams, it attempts to bait the receiver to take action (opening a link or attachment) with a consequence for failing to do so (disabling the account). The links or attachment may be set up to steal information or to download malware onto the tax professional's computer. In this case, the tax preparers are being asked to

because there are so many remote transactions during the pandemic. The thief may interact repeatedly with a tax professional and then send an email with an attachment that claims to include their tax information.

The attachment may contain malware that allows the thief to track keystrokes and eventually steal all passwords or take over control of the computer systems.

Some phishing scams are ransomware schemes in which the thief gains control of the tax professionals' computer systems and holds the data hostage until a ransom is paid. The Federal Bureau of Investigation (FBI) has warned against paying a ransom because thieves often leave the data encrypted.

The need for a security plan and data theft plan

The IRS and Security Summit partners remind tax professionals that federal law requires them to have a written information security plan. In addition to the required information security plan, tax pros also should consider an emergency response plan should they experience a breach and data theft. This time-saving step should include contact information for the IRS Stakeholder Liaisons, who are the first point of contact for data theft reporting to the IRS and to the states.

IRS Publication 5293, Data Security Resource Guide for Tax Professionals PDF, provides a compilation of data theft information available on IRS.gov, including the reporting processes.

The IRS, state tax agencies, the private sector tax industry – including tax professionals – work in partnership as the Security Summit to help protect taxpayers from identity theft and refund fraud. This is the fourth in a week-long series of tips to raise awareness about identity theft.

Technology