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: Tax pros should remain vigilant against phishing emails and cloud-based attacks

IR-2023-138, Aug. 1, 2023

WASHINGTON – In the third installment of a special series, the Security Summit partners warned tax professionals to be aware of evolving phishing scams and cloud-based schemes designed to steal sensitive taxpayer information.

The IRS and its Security Summit partners - state tax agencies and the nation's tax industry – continue to see a steady stream of attacks aimed at the nation's tax professional community to steal sensitive tax and financial information from clients.

"We continue to see a relentless string of attempts from scammers to obtain sensitive tax professional information," said IRS Commissioner Danny Werfel. "Identity thieves and fraudsters continue to look for new and inventive ways into tricking tax pros. These scams can be subtle and sophisticated, and tax pros should not let down their guard to protect their clients and their businesses."

This is the third release in a five-part "Protect Your Client; Protect Yourself" summer series from the Security Summit, a public-private partnership that works to protect the tax system against tax-related identity theft and fraud.

The weekly news release series and the IRS Nationwide Tax Forums, which continue later this month in Washington, D.C., San Diego and Orlando, provide important information to help protect sensitive taxpayer data that tax professionals hold while also protecting their business from identity thieves. This marks the eighth year that the Security Summit partners have worked to raise awareness about these issues through the "Protect Your Clients; Protect Yourself" campaign.

Phishing, spear phishing and whaling

One of the most common threats facing tax pros are f phishing and related scams. These are designed to trick the recipient into disclosing personal information such as passwords, bank account numbers, credit card numbers or Social Security numbers.

Tax professionals and taxpayers should be aware of different phishing terms and what the scams might look like:

- **Phishing/Smishing** – Phishing emails or SMS/texts (known as "smishing") attempt to trick the recipient into clicking a suspicious link, filling out information or downloading a malware file. Often phishing attempts are sent to multiple email addresses at a business or agency increasing the chance someone will fall for the trick.

- **Spear phishing** – A specific type of phishing scam that bypasses emailing large groups at an organization, but instead identifies potential victims and delivers a more realistic email known as a "lure." These types of scams can be trickier to identify since they don't occur in large numbers. They single out individuals, can be specialized and make the email seem more legitimate. These can pose as a potential client for a tax professional, luring the practitioner into sharing sensitive information.

- **Whaling** – Whaling attacks are very similar to spear phishing, except these attacks are generally targeted to leaders or other executives with access to secure large amounts of information at an

organization or business. Whaling attacks can also target people in payroll offices, human resource personal and financial offices.

Security Summit partners continue to see instances where tax professionals have been particularly vulnerable to emails posing as potential clients. The criminals use this technique to trick practitioners into opening email links or attachments that infect computer systems with the potential to steal client information. Similar schemes are seen with whaling situations where scammers try to obtain large amount of information with legitimate looking email requests.

“The complexity and realism of all these schemes can really catch tax pros and many others off-guard,” Werfel said. “Scammers can be quite creative and resourceful. We urge the tax community to remain vigilant as well as taxpayers and anyone else with sensitive financial information.”

Warning signs of scams

Regardless of the type of phishing attempt, tax pros can protect themselves or their organization by being aware of these scams and looking for warning signs like:

- An unexpected email or text claiming 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.
- A false narrative often with an urgent tone urging the receiver to open a link or attachment.
- An email address, number or link that’s misspelled or has a different domain name or URL (*irs.**com** vs. IRS.**gov**).*

Cloud-based schemes can ruin a summer day

Tax professionals using cloud-based systems that store information or run tax preparation software should use multi-factor authentication to help safeguard that data.

Specifically, the Security Summit continues to see attacks that take advantage of cloud-based systems and compromise personal information. Multi-factor authentication options provide an additional layer of security to access a system by using a phone, text messages or tokens. Since email is easier for identity thieves to access, having these layers of security helps guard against potential vulnerabilities.

Additional Resources

For tax professionals who are victim of any of these schemes or identity theft, IRS urges them to quickly contact their IRS Stakeholder Liaison to provide details of the situation. Quickly reporting these incidents can not only protect the tax pro’s clients, it can also help provide critical information timely that can help prevent these attacks from hitting others in the tax community.

Tax professionals should review IRS Publication 4557, Safeguarding Taxpayer Data, for more information.

Other resources include Small Business Information Security: The Fundamentals, by the National Institute of Standards and Technology and the IRS’ Identity Theft Central pages for tax pros.

Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation of data theft information available on IRS.gov. The IRS also encourages tax professionals to stay connected to the IRS for its latest updates and alerts through subscriptions to e-News for Tax Professionals and its social media sites.

-30-