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

New, evolving scams threaten tax professionals; Security Summit warns extra attention needed on trending threats that could affect businesses, clients

Week 1 of "Protect Your Clients; Protect Yourself" series focuses on new and old scams, schemes

IR-2024-183, July 9, 2024

WASHINGTON – The Internal Revenue Service and the Security Summit renewed a warning today to tax professionals to be on the lookout for a variety of new and evolving schemes aimed at stealing business and taxpayer information.

Identity thieves are taking numerous approaches to steal sensitive information from tax professionals. This includes posing as new clients; using phishing emails to trick people into sharing Central Authorization File information as well elaborate schemes involving calling and texting. Tax professionals need to be on the lookout to avoid falling prey to these attacks, which threaten not just their clients but their businesses.

"As the Security Summit partners have continued to improve our defenses against identity theft, thieves have upped their game by targeting tax professionals to get valuable information needed to file authentic-looking tax returns," IRS Commissioner Danny Werfel said. "Tax professionals need to watch out for deviously clever scams that can masquerade as new clients as well as communications from the IRS or others in the tax community. We continue to see tax professionals bombarded by these scams, and people shouldn't let their defenses down."

The alert comes as part of an annual education effort by the Security Summit partners, a coalition of tax professionals, industry partners, state tax groups and the IRS. Started in 2015, the public-private partnership works to protect the tax system against tax-related identity theft and fraud.

This marks the opening week of a special Security Summit summer news release series called "Protect Your Clients; Protect Yourself." The campaign is aimed at increasing awareness among tax professionals on ways to shield themselves and their clients from identity theft and security threats.

Now in its ninth year, the "Protect Your Clients; Protect Yourself" series will feature news releases each Tuesday for eight weeks. The series coincides with the Nationwide Tax Forum, a three-day seminar starting today in Chicago and continues with sessions the week of July 30 in Orlando, August 13 in Baltimore, August 20 in Dallas and September 10 in San Diego. The IRS reminds tax pros that registration deadlines are quickly approaching for several of the forums, and Chicago and Orlando are already sold out.

The IRS forums will feature several specific sessions to help educate the tax professional community on security-related topics. Tax professionals will hear from experts at the IRS, the tax professional community as well as a special session from the Salve Regina University's Pell Center from Rhode Island. The entire news release series will be available in Spanish as well.

As part of this effort, the IRS and Security Summit partners are warning against the most recent wave of activity coming from tax scammers. Here are some trending examples that tax professionals should watch out for:

Beware of the "new client" scheme

In this form of so-called spear phishing, fraudsters pretend to be real taxpayers seeking tax pros' help

with their taxes. They use emails to try to get sensitive information or gain access to a practitioner's client data. In these fake "new client" schemes, the fraudster can send a malicious attachment or include a link to a site that the tax professional thinks they need to access to obtain the supposed new client's tax information. But in reality, the site is collecting information from the tax pro, such as their email and password, or loading malware onto the tax pro's computer to gain access to their computer or system.

While not a fresh scam, the IRS continues seeing activity this year. It remains an ongoing threat that can be alluring to a tax professional or a practice's employees seeking new business. And while this fake outreach can peak around tax season, this sort of scam remains a threat year-round.

Look out for multiple phishing scams involving EFINs, PTINs, CAF numbers

Another scam circulating on a large scale this year involves phishing attempts by scammers trying to obtain various identification numbers used by tax professionals, including their Electronic Filing Identification Number or EFIN; EFIN documents; their Preparer Tax Identification Number or PTIN; and their Centralized Authorized File or CAF number.

Obtaining these digits helps a bad actor obtain information and file a fraudulent return that looks legitimate. Scammers are trying to get these sensitive identification numbers by sending emails or texts that appear to be from the IRS. The scammers tell tax pros they need to confirm this information by entering it into a form that was hosted on what appears to be a real IRS website, but in reality is a fake website designed to mimic the real thing.

For example, a fraudster with a compromised CAF number in hand can use it to obtain tax transcripts and other sensitive taxpayer personally identifiable information (PII) to commit identity theft refund fraud and other crimes. In many cases, the fraudster has not only obtained a practitioner's CAF number but also has the tax professional's sensitive personal information.

Watch and listen for phone, text and correspondence schemes

Tax professionals should also be aware of another wave of scams hitting taxpayers with frequency, with identity thieves using phone calls and text messages to get Social Security numbers, birth dates and banking information from victims. Several of these schemes are common right now that can target not just taxpayers, but potentially tax professionals and their clients, including:

- Artificial intelligence or AI scams used for false correspondence, with AI being used to create fake IRS letters that are mailed to victims.
- The so-called Zero Tax program, in which callers promise to wipe out tax debt for people who owe back taxes. The callers request people's Social Security numbers as part of their pitch, which they use for nefarious purposes. Tax professionals should watch out for clients reporting this scheme.
- Social media scams circulating inaccurate or misleading tax information that can involve creating common tax documents that are false like a Form W-2 or claiming credits to which the taxpayer is not entitled like the Fuel Tax Credit, Sick and Family Leave Credit and household employment credits.
- Scammers reaching out by phone or text message to dupe people into handing over sensitive financial information in exchange for a false promise of IRS money for them.

Ways to avoid and report scams

People that receive scams by email should send the email to phishing@irs.gov. As a reminder, people can forward the message, but IRS cybersecurity experts prefer to see the full email header to help them identify the scheme.

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

For tax professionals who discover they are victims of a security breach, they should contact their IRS Stakeholder Liaison to report a theft. The local IRS Stakeholder Liaison will ensure the appropriate IRS offices are alerted. If incidents are reported quickly, the IRS can take steps to block fraudulent returns in the clients' names and will assist tax pros through the process.

Tax professionals can also share information with the appropriate state tax agency by visiting a special "Report a Data Breach" page with the Federation of Tax Administrators.

Tax professionals should also understand the Federal Trade Commissioner data breach response requirements as part of their overall information and data security plan. The new Written Information Security Plan, or WISP, that tax pros are required to have also notes there's a new requirement to report an incident to the FTC when 500 or more people are affected within 30 days of the incident.

-30-