PRODUCT & SERVICE GUIDE

Tax Pros Being Hit with New Phishing Scam, Putting Client Data at Risk

In recent days, the “New Client” scam has re-emerged, signaling ongoing attempts by cybercriminals to target tax professionals with spear phishing schemes. In this scam, a “new client” emails the tax pro about a tax issue, attaching documents to their ...

Mar. 23, 2018
Tax professionals are being warned about a new scam that can result in taxpayer data theft in the final weeks of the tax filing season. The IRS, state tax agencies and software companies serving tax prepares convened at a Security Summit, and are urging tax professionals to enhance their data safeguards immediately.

In recent days, the “New Client” scam has re-emerged, signaling ongoing attempts by cybercriminals to target tax professionals with spear phishing schemes. In this scam, a “new client” emails the tax pro about a tax issue, attaching documents to their email that they claim to be an IRS notice or prior-year tax information. The documents actually contain malware that, if opened, enable the criminals to steal taxpayer information.

This filing season, the IRS has seen a steep upswing in the number of reported thefts of taxpayer data from tax practitioner offices. Seventy-five firms reported taxpayer data thefts in January and February, nearly a 60 percent increase from the same time last year. Much of this increase follows one scam, the erroneous refund scheme, that affected thousands of taxpayers and numerous practitioners earlier this filing season.

January through April represents prime season for cybercriminals to attack tax practitioners, but data thefts can occur at any time. Tax professionals should be on
high alert and deploy strong security measures as the filing season reaches a peak with the April 17 deadline approaching. Criminals try to take advantage of this extremely busy time of year when tax professionals are in greater contact with taxpayers and are therefore in possession of more data.

Some tax professionals may be unaware they are victims of data theft. Here are some signs:

- Client e-filed returns begin to reject because returns with their Social Security numbers were already filed;
- The number of returns filed with tax practitioner’s Electronic Filing Identification Number (EFIN) exceeds number of clients;
- Clients who haven’t filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS;
- Network computers running slower than normal;
- Computer cursors moving or changing numbers without touching the keyboard;
- Network computers locking out tax practitioners.

Identity thieves often are part of sophisticated criminal syndicates based in the U.S. and abroad. These syndicates are resourceful, being tax savvy and having digital expertise to pull off these crimes. They use a variety of tactics to break into tax professionals’ computer systems and steal client information if appropriate security measures have not been taken.

A common tactic, called spear phishing, occurs when the criminal singles out one or more tax preparers in a firm and sends an email posing as a trusted source such as the IRS, e-Services, a tax software provider or a cloud storage provider. Thieves also may pose as clients or new prospects. The objective is to trick the tax professional into disclosing sensitive usernames and passwords or to open a link or attachment that secretly downloads malware enabling the thieves to track every keystroke.

The “New Client” scam is one form of spear phishing. Here’s an example: “I just moved here from Michigan. I have an urgent Tax issue and I was hoping you could help,” the email begins. “I hope you are taking on new clients.” The email says one attachment is the IRS notice and the other attachment is the prospective client’s prior-year tax return. This scam has many variations. (See IR-2018-2, Security Summit Partners Warn Tax Pros of Heightened Fraud Activity as Filing Season Approaches.)
The IRS Criminal Investigation Division continues to investigate a series of data thefts at tax preparers’ offices that occurred earlier this year in which the criminals added a new twist to their scheme to file fraudulent tax returns. The thieves directed the fraudulent refunds into the taxpayers’ actual bank accounts. This scam has claimed thousands of taxpayer victims. (See IR-2018-17, Scam Alert: IRS Urges Taxpayers to Watch Out for Erroneous Refunds.)

Although reports of this data theft have lessened recently, taxpayers and tax professionals should remain on alert for this scam. Taxpayers should return any fraudulent refunds to the IRS as well as discuss security options for their checking or savings accounts with their financial institutions. Here are the recommended security steps by the Security Summit:

- Learn to recognize phishing emails, especially those pretending to be from the IRS, e-Services, a tax software provider or cloud storage provider. Never open a link or any attachment from a suspicious email. Remember: The IRS never initiates contact via email.
- Create a data security plan using IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security – The Fundamentals, by the National Institute of Standards and Technology.
- Review internal controls:
  - Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets and phones) and keep software set to automatically update.
  - Use strong and unique passwords of 10 or more mixed characters, password protect all wireless devices, use a phrase or words that are easily remembered and change passwords periodically.
  - Encrypt all sensitive files/emails and use strong password protections.
  - Back up sensitive data to a safe and secure external source not connected fulltime to a network.
  - Wipe clean or destroy old computer hard drives that contain sensitive data.
  - Limit access to taxpayer data to individuals who need to know.
  - Check IRS e-Services account weekly for number of returns filed with EFIN.
- Those who experience a security incident or a breach resulting in data disclosure should report the incident to the appropriate IRS Stakeholder Liaison.
CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2022 Firmworks, LLC. All rights reserved