never sent. If a practitioner mistakenly provides username and password information to the ...

Aug. 08, 2019

The Internal Revenue Service and its Security Summit partners are urging tax professionals to learn the tell-tale signs that their office may have experienced a data theft that resulted in fraudulent tax returns being filed in their clients' names.

The IRS, state tax agencies and the private-sector tax industry, working together as the Security Summit, warned practitioners that global criminal syndicates remain active, and they are well financed, high skilled and tax savvy in their attempts to gain sensitive tax data.

The reminder came as the IRS and the Summit partners encouraged tax professionals

Recognizing the signs of data theft is the fourth item on the "Taxes-Security-Together" Checklist. Previous checklist items include: deploying the "Security Six" basic steps, creating a written data security plan and educating yourself on email phishing scams.

Although the Security Summit — a partnership between the IRS, states and the private-sector tax community started in 2015 — is making major progress against tax-related identity theft, cybercriminals continue to quickly evolve, and data thefts at tax professionals' offices remain a major attack point. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder for Summit partners to detect.

Recognize the signs of client data theft

The IRS and Summit partners have created a list of warning signs that a tax professional or their office may have experienced a data theft:

- Client e-filed returns begin to be rejected by the IRS or state tax agencies because returns with their Social Security numbers were already filed;
- Clients who haven't filed tax returns begin to receive taxpayer authentication letters (5071C, 4883C, 5747C) from the IRS to confirm their identity for a submitted tax return.
- Clients who haven't filed tax returns receive refunds;
- Clients receive tax transcripts that they did not request;
- Clients who created an IRS Online Services account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled. Another variation: Clients unexpectedly receive an IRS notice that an IRS online account was created in their names;

- The number of returns filed with the tax professional's Electronic Filing

Because IRS and state tax systems will only accept one unique Social Security number, taxpayers often discover they are a victim when they attempt to e-file and their tax return is rejected because a return with their SSN already is in the system. Or, more commonly, the IRS identifies a return that could be an identity theft return and sends a letter to the taxpayer asking them to contact the agency to let the IRS know if they filed the return.

Identity thieves sometimes try to leverage the stolen data by using taxpayer information to access the IRS Get Transcript system. Taxpayers who receive transcripts by mail but did not order them are sometimes victims of this approach. Get Transcript Online is protected by a robust, two-factor authentication process. But crooks may still try to use stolen identities to try to create Get Transcript accounts, which results in the IRS disabling the account and sending the taxpayer a letter.

During the tax filing season, tax professionals should make a weekly review of returns filed with the office's Electronic Filing Identification Number, or EFIN. A report is updated weekly. Tax preparers can access their e-File applications and select "check EFIN status" to see a count. If the numbers are inflated, practitioners should contact the IRS e-Help Desk.

Tax professionals may also notice IRS acknowledgements for returns they did not e-file. Acknowledgements are sent soon after a return is transmitted.

Tax professionals who fall victim to spear phishing email scams, a common way cybercriminals access office computer, may suddenly see responses to emails they never sent. If a practitioner mistakenly provides username and password information to the thief, the thief often harvests the practitioner's contact list,

stealing names and email addresses of colleagues and clients and enabling the crooks

to practitioners' office computers, complete the pending Form 1040s, change electronic deposit information to their own accounts and then e-filed the returns – all performed remotely.

Tax professionals who notice any signs of identity theft should contact their state's IRS Stakeholder Liaison immediately. The process for reporting data theft to the IRS is outlined in Data Theft Information for Tax Professionals.

In some states, data thefts must be reported to various authorities. To help tax professionals find where to report data security incidents at the state level, the Federation of Tax Administrators has created a special page with state-by-state listings.

CPA Practice Advisor 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.