THETAXBOOK News Release Date: 2/6/18

IRS Warns of New Debt Collector Scam

Cross References

- IR-2018-17, February 2, 2018

Seeing the emergence of a new filing season scam, the IRS is urging tax professionals to step up security and beware of phishing emails that can secretly download malicious software that can help cybercriminals steal client data.

Only a few days into the filing season, the IRS has already identified a new scam that began with cybercriminals stealing data from several tax practitioners' computers and filing fraudulent tax returns.

In a new twist, the fraudulent returns in a few cases used the taxpayers' real bank accounts for the deposit. A woman posing as a debt collection agency official then contacted the taxpayers to say a refund was deposited in error and asked the taxpayers to forward the money to her.

This scheme is likely just the first of many that will be identified this year as the IRS, state tax agencies and tax industry continue to fight back against tax-related identity thieves. Because the Security Summit partners have made inroads against identity theft, cybercriminals have evolved their tactics to focus on tax professionals where they can steal client data.

Thieves know it is more difficult to identify and halt fraudulent tax returns when they are using real client data such as income, dependents, credits and deductions. Generally, criminals find alternative ways to get the fraudulent refunds delivered to themselves rather than the real taxpayers.

Tax professionals are reminded that there is a procedure for them to report data thefts to the IRS. They need only contact their state's IRS Stakeholder Liaison, who will notify appropriate IRS officials and serve as a point of contact.

IRS Criminal Investigation agents are still reviewing this latest data theft scam. However, the vast majority of data thefts occur because the tax preparer or someone in the office opened a phishing email and clicked on a link or attachment that contained malware. There are various forms of malware but some download secretly into computers and allow thieves to see each keystroke or give thieves remote access to computers. Both versions allow thieves to steal data stored on the computers.

Tax professionals are urged to seek cybersecurity experts to help better secure their data. Here's a reminder of some basic steps tax professionals can take:

- Educate all employees about phishing in general and spear phishing in particular.
- Use strong, unique passwords. Use a phrase instead of a word. Use different passwords for each account. Use a mix of letters, numbers and special characters.

- Never take an email from a familiar source at face value; example: an email from "IRS e-Services." If it asks you to open a link or attachment, or includes a threat to close your account, think twice. Visit the e-Services website for confirmation.
- If an email contains a link, hover your cursor over the link to see the web address (URL) destination. If it's not a URL you recognize or if it's an abbreviated URL, don't open it.
- Consider a verbal confirmation by phone if you receive an email from a new client sending you tax information or a client requesting last-minute changes to their refund destination.
- Use security software to help defend against malware, viruses and known phishing sites and update the software automatically.
- Use the security options that come with your tax preparation software.
- Send suspicious tax-related phishing emails to phishing@irs.gov.

This newest scam also serves as a reminder to taxpayers that they should be alert to any unusual activity such as receiving a tax transcript or tax refund they did not request.

Taxpayers who receive a direct deposit refund that they did not request should take the following steps:

1) Contact the Automated Clearing House (ACH) department of the bank/financial institution where the direct deposit was received and have them return the refund to the IRS.
2) Call the IRS toll-free at 800-829-1040 (individual) or 800-829-4933 (business) to explain why the direct deposit is being returned.
3) Keep in mind interest may accrue on the erroneous refund.