THETAXBOOK News Release Date: 3/6/2019

Refund Scams

Cross References

• IR-2018-27

The IRS is warning taxpayers of a quickly growing scam involving erroneous tax refunds being deposited into their bank accounts. After stealing client data from tax professionals and filing fraudulent tax returns, the scammer uses the taxpayer's real bank accounts for the deposit. Various tactics are then used to reclaim the refund from the taxpayer.

In one version, the scammer posing as a debt collection agency official acting on behalf of the IRS contacts the taxpayer and says a refund was deposited in error, and asks the taxpayer to forward the money to their collection agency.

In another version, the taxpayer who received the erroneous refund gets an automated call with a recorded voice saying he is from the IRS and threatens the taxpayer with criminal fraud charges, an arrest warrant, and a blacklisting of their Social Security Number. The recorded voice gives the taxpayer a case number and a telephone number to call to return the refund.

The IRS has an established procedure for returning an erroneous refund to the agency. The IRS also encourages taxpayers to discuss the issue with their financial institutions because there may be a need to close a bank account.

If the erroneous refund was a direct deposit, contact the Automated Clearing House (ACH) department of the bank or financial institution where the direct deposit was received and have them return the refund to the IRS. Then call the IRS at 800-829-1040 for individuals, or 800-829-4933 for businesses, to explain why the direct deposit is being return.

If the erroneous refund was a paper check, see the IRS scam alert website (https://www.irs.gov/newsroom/) for instructions.

If an e-filed return is rejected because a return bearing the taxpayer's Social Security Number is already on file, follow the steps outlined in the Taxpayer Guide to Identity Theft, posted on the IRS website (https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft). Taxpayers unable to file electronically should mail a paper tax return along with Form 14039, *Identity Theft Affidavit,* stating they were victims of a tax preparer data breach.

The IRS also urges tax professionals to be on high alert to unusual activity. Criminals increasingly target tax professionals, deploying various types of phishing emails in an attempt to access client data. Thieves then use this data to impersonate taxpayers and file fraudulent tax returns for refunds. Tax practitioners should not communicate solely by email with potential or existing clients, especially if unusual requests are made.

Author's Comment

I have a separate dedicated laptop computer that is exclusively used for tax preparation. I have a second computer that is used for web browsing, email correspondence, and other non-tax preparation related use. Client data is stored only on the tax preparation laptop and external hard drive backups. The other computer contains no client data or client information on its hard drive. The tax preparation laptop and backup hard drives are turned off and locked up when not in use. I have a "no click" policy, meaning under no circumstance do I click on an email attachment or link, even if I think I know who the sender is. I call the client and have them send their information by snail mail if they cannot personally hand deliver their tax information. Using two computers is cheaper and easier than trying to deal with a data breach or client identity theft.