THE TAXBOOK News
Release Date: 3/6/18

Phishing Schemes Make IRS Dirty Dozen List of Tax Scams

Cross References

- IR-2018-39, March 5, 2018

Following continuing threats to taxpayers, the IRS has listed email phishing schemes as a top filing season concern and part of the annual listing of the Dirty Dozen tax scams for 2018.

The IRS warned taxpayers, businesses, and tax professionals to be alert to fake emails or websites looking to steal personal information. These attempts can expand during tax season and remain a major identity theft threat.

Compiled annually by the IRS, the Dirty Dozen lists a variety of common scams that taxpayers may encounter any time of the year, but many of these schemes peak during filing season as people prepare their tax returns or seek help from tax professionals.

To help protect taxpayers, the IRS is highlighting each of these scams on 12 consecutive days to help raise awareness. The IRS also urges taxpayers to help protect themselves against identity theft by reviewing safety tips prepared the Security Summit, a collaborative effort between the IRS, states and the private-sector tax community.

"We urge taxpayers to watch out for these tricky and dangerous schemes," said Acting IRS Commissioner David Kautter. "Phishing and other scams on the Dirty Dozen list can trap unsuspecting taxpayers. Being cautious and taking basic security steps can help protect people and their sensitive tax and financial data."

2018 Sees New Phishing Schemes

The IRS continues to see a steady onslaught of new and evolving phishing schemes as scam artists work to victimize taxpayers during filing season.

In a recent twist to a phishing scam, the IRS has seen thousands of taxpayers victimized by an unusual scheme that involves their own bank accounts. After stealing client data from tax professionals and filing fraudulent tax returns, the criminals use taxpayers' real bank accounts to direct deposit refunds. Thieves are then using various tactics to reclaim the refund from the taxpayers, including falsely claiming to be from a collection agency or representing the IRS. Phone calls, emails, and websites are used to make the scheme more elaborate. Versions of the scam may continue to evolve. The IRS encourages taxpayers to review some basic tips if they see an unexpected deposit in their bank account.

In addition, the IRS has seen email schemes in recent weeks targeting tax professionals, payroll professionals, human resources personnel, schools, as well as individual taxpayers.

In these email schemes, criminals pose as a person or organization the taxpayer trusts or recognizes. They may hack an email account and send mass emails under another person's name. Or they may pose as a bank, credit card company, tax software provider, or government agency. Criminals go to great lengths to create websites that appear legitimate but contain phony log-in pages. These criminals hope victims will take the bait and provide money, passwords, Social Security numbers and other information that can lead to identity theft.

Fake emails and websites also can infect a taxpayer's computer with malware without the user knowing it. The malware gives the criminal access to the device, enabling them to access all sensitive files or even track keyboard strokes, exposing login information.

For those participating in these schemes, such activity can lead to significant penalties and possible criminal prosecution. IRS Criminal Investigation works closely with the Department of Justice to shutdown scams and prosecute the criminals behind them.

Tax Pro Alert

Numerous data breaches in the past year mean the entire tax preparation community must be on high alert during filing season to any unusual activity. Criminals increasingly target tax professionals, deploying various types of phishing emails in an attempt to access client data. Thieves may use this data to impersonate taxpayers and file fraudulent tax returns for refunds.

As part of the Security Summit initiative, the IRS has joined with representatives of the software industry, tax preparation firms, payroll and tax financial product processors and state tax administrators to combat identity theft refund fraud to protect the nation's taxpayers.

The Security Summit partners encourage tax practitioners to be wary of communicating solely by email with potential or even existing clients, especially if unusual requests are made. Data breach thefts have given thieves millions of identity data points including names, addresses, Social Security numbers and email addresses. If in doubt, tax practitioners should call to confirm a client's identity.

What to Do With Phishing Attempts

If a taxpayer receives an unsolicited email that appears to be from either the IRS or an organization closely linked to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), they should report it by sending it to phishing@irs.gov. Learn more by going to the Report Phishing and Online Scams page on IRS.gov.

Tax professionals who receive unsolicited and suspicious emails that appear to be from the IRS or related to the e-Services program also should report it by sending it to phishing@irs.gov.

It is important to keep in mind the IRS generally does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.