IRS Kicks Off Annual List of Most Prevalent Tax Scams:
Agency Warns Taxpayers of Pervasive Phishing Schemes in its 'Dirty Dozen' Campaign

IR-2019-26, March 4, 2019

WASHINGTON — Kicking off the annual "Dirty Dozen" list of tax scams, the Internal Revenue Service today warned taxpayers of the ongoing threat of internet phishing scams that lead to tax-related fraud and identity theft.

The IRS warns taxpayers, businesses and tax professionals to be alert for a continuing surge of fake emails, text messages, websites and social media attempts to steal personal information. These attacks tend to increase during tax season and remain a major danger of identity theft.

To help protect taxpayers against these and other threats, the IRS highlights one scam on 12 consecutive week days to help raise awareness. Phishing schemes are the first of the 2019 "Dirty Dozen" scams. "Taxpayers should be on constant guard for these phishing schemes, which can be tricky and cleverly disguised to look like it's the IRS," said IRS Commissioner Chuck Rettig. "Watch out for emails and other scams posing as the IRS, promising a big refund or personally threatening people. Don't open attachments and click on links in emails. Don't fall victim to phishing or other common scams."

The IRS also urges taxpayers to learn how to protect themselves by reviewing safety tips prepared by the Security Summit, a collaborative effort between the IRS, state revenue departments and the private-sector tax community.

"Taking some basic security steps and being cautious can help protect people and their sensitive tax and financial data," Rettig said.

New Variations on Phishing Schemes

The IRS continues to see a steady stream of new and evolving phishing schemes as criminals work to victimize taxpayers throughout the year. Whether through legitimate-looking emails with fake, but convincing website landing pages, or social media approaches, perhaps using a shortened URL, the end goal is the same for these con artists: stealing personal information.

In one variation, taxpayers are victimized by a creative scheme that involves their own bank account. After stealing personal data and filing fraudulent tax returns, criminals use taxpayers' bank accounts to direct deposit tax refunds. Thieves then use various tactics to reclaim the refund from the taxpayer, including falsely claiming to be from a collection agency or the IRS. The IRS encourages taxpayers to review some basic tips if they see an unexpected deposit in their bank account.

Schemes Aimed at Tax Pros, Payroll Offices, Human Resources Personnel

The IRS has also seen more advanced phishing schemes targeting the personal or financial information available in the files of tax professionals, payroll professionals, human resources personnel, schools and organizations such as Form W-2 information. These targeted scams are known as business email compromise (BEC) or business email spoofing (BES) scams.

Depending on the variation of the scam (and there are several), criminals will pose as:

- a business asking the recipient to pay a fake invoice
- as an employee seeking to re-route a direct deposit
- or as someone the taxpayer trusts or recognizes, such as an executive, to initiate a wire transfer.

The IRS warned of the direct deposit variation of the BEC/BES scam in December 2018, and continues to receive reports of direct deposit scams reported to phishing@irs.gov. The Direct Deposit and other BEC/BES variations should be forwarded to the Internet Crime Complaint Center (IC3). The IRS requests that Form W-2 scams be reported to: phishing@irs.gov (Subject: W-2 Scam).

Criminals may use the email credentials from a successful phishing attack, known as an email account compromise, to send phishing emails to the victim's email contacts. Tax preparers should be wary of unsolicited email from personal or business contacts especially the more commonly observed scams, like new client solicitations.

Malicious emails and websites can infect a taxpayer's computer with malware without the user knowing it. The malware downloads in the background, giving the criminal access to the device, enabling them to access any sensitive files or even track keyboard strokes, exposing login victim's information.

For those participating in these schemes, such activity can lead to significant penalties and possible criminal prosecution. Both the Treasury Inspector General for Tax Administration (TIGTA), which handles scams involving IRS impersonation, and the IRS Criminal Investigation Division work closely with the Department of Justice to shut down scams and prosecute the criminals behind them.

Tax Professional Alert

Numerous data breaches across the country mean the tax preparation community must be on high alert to unusual activity, particularly during the tax filing season. 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 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.

Reporting Phishing Attempts

If a taxpayer receives an unsolicited email or social media attempt 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 and/or are tax-related (like those related to the e-Services program) also should report it to: phishing@irs.gov. 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.