THE TAXBOOK News
Release Date: 7/10/23

IRS Warns Taxpayers About Refund Scam

Cross References

- IR-2023-123, July 3, 2023

The Internal Revenue Service is warning taxpayers to be on the lookout for a new scam mailing that tries to mislead people into believing they are owed a refund.

The new scheme involves a mailing coming in a cardboard envelope from a delivery service. The enclosed letter includes the IRS masthead and wording that the notice is "in relation to your unclaimed refund."

Like many scams, the letter includes contact information and a phone number that do not belong to the IRS. But it also seeks a variety of sensitive personal information from taxpayers—including detailed pictures of driver's licenses—that can be used by identity thieves to try obtaining a tax refund and other sensitive financial information.

"This is just the latest in the long string of attempts by identity thieves posing as the IRS in hopes of tricking people into providing valuable personal information to steal identities and money, including tax refunds," said IRS Commissioner Danny Werfel. "These scams can come in through email, text or even in special mailings. People should be careful to watch out for red flags that clearly mark these as IRS scams."

The Security Summit—a coalition between the IRS, state tax administrators and the nation's tax industry—continue to warn people to protect their personal information to protect against tax-related identity theft as well as scams like this.

In this new scam, there are many warning signs that can be seen in many similar schemes via email or by text. An unusual feature of this scam is that it tries tricking people to email or phone very detailed personal information in hopes of stealing valuable information.

The letter tells the recipients they need to provide "Filing Information" for their refund. This includes some awkwardly worded requests like this:

"A Clear Phone of Your Driver's License That Clearly Displays All Four (4) Angles, Taken in a Place with Good Lighting."

The letter proceeds for more sensitive information including cellphone number, bank routing information, Social Security number and bank account type, followed by a poorly worded warning:

"You'll Need to Get This to Get Your Refunds After Filing. These Must Be Given to a Filing Agent Who Will Help You Submit Your Unclaimed Property Claim. Once You Send All The Information Please Try to Be Checking Your Email for Response From The Agents Thanks"

This letter contains a variety of warning signs, including odd punctuation and a mixture of fonts as well as inaccuracies.

For example, the letter states the deadline for filing tax refunds is October 17; the deadline for people on extension for their 2022 tax returns is actually October 16, and those owed refunds from last year have time beyond that. And the IRS handles tax refunds, not "unclaimed property."

Important reminders about scams. The IRS and Security Summit partners regularly warn people about common scams, including the annual IRS Dirty Dozen list.

Taxpayers and tax professionals should be alert to fake communications posing as legitimate organizations in the tax and financial community, including the IRS and states. These messages can arrive in the form of an unsolicited text or email to lure unsuspecting victims to provide valuable personal and financial information that can lead to identity theft, including phishing and smishing.

The IRS never initiates contact with taxpayers by email, text or social media regarding a bill or tax refund.

As a reminder: Never click on any unsolicited communication claiming to be the IRS as it may surreptitiously load malware. It may also be a way for malicious hackers to load ransomware that keeps the legitimate user from accessing their system and files.

Individuals should never respond to tax-related phishing or smishing or click on the URL link. Instead, the scams should be reported by sending the email or a copy of the text/SMS as an attachment to phishing@irs.gov. The report should include the caller ID (email or phone number), date, time and time zone, and the number that received the message.

Taxpayers can also report scams to the Treasury Inspector General for Tax Administration or the Internet Crime Complaint Center. The Report Phishing and Online Scams page at IRS.gov provides complete details. The Federal Communications Commission's Smartphone Security Checker is a useful tool against mobile security threats.

The IRS also warns taxpayers to be wary of messages that appear to be from friends or family but that are possibly stolen or compromised email or text accounts from someone they know. This remains a popular way to target individuals and tax preparers for a variety of scams. Individuals should verify the identity of the sender by using another communication method; for instance, calling a number they independently know to be accurate, not the number provided in the email or text.