THE TAXBOOK News
Release Date: 8/2/23

Summer Wave of Email and Text Scams

Cross References

- IR-2023-131

The Internal Revenue Service is warning taxpayers to be on the lookout for a summer surge of tax scams as identity thieves continue pounding out a barrage of email and text messages promising tax refunds or offers to help 'fix' tax problems.

The latest email schemes touch on a variety of topics, but many center around promises about a third round of Economic Impact Payments. The IRS is seeing hundreds of complaints daily pouring into phishing@irs.gov about this scam, which has an embedded URL link that takes people to phishing website to steal sensitive taxpayer information.

The IRS is also receiving reports of emails urging people to "Claim your tax refund online," and text messages that the person's tax return was "banned" by the IRS. These scams are riddled with spelling errors and awkward phrasing, but they consistently try to entice people to click on a link.

"The IRS is seeing a wave of these summer scams relentlessly pounding taxpayers," said IRS Commissioner Danny Werfel. "People are being flooded with these email and text messages, but we want them to avoid getting swept up in these terrible scams. Taxpayers should be wary; remember, don't click on links from questionable sources."

As part of the Security Summit effort, the IRS has been working in partnership with state tax administrators, tax professionals and the nation's tax industry to warn people about identity theft risks, including the ongoing push by scammers to trick people into sharing personal information through email, texts and phone calls. The Security Summit is currently in the middle of a special summer news release series aimed increasing awareness among tax professionals on ways to protect themselves, and their clients, against identity theft.

At the same time, the IRS and Security Summit continue to warn taxpayers against the most recent wave of activity involving tax scammers. Here are some highlights.

The Economic Impact Payment scheme. This is currently the highest volume email scheme the IRS is seeing. Email messages are hitting inboxes with titles like: "Third Round of Economic Impact Payments Status Available." The IRS routinely sees hundreds of taxpayers forwarding these messages each day; the IRS has seen thousands of these emails reported since the July 4 holiday period.

The third round of Economic Impact Payments occurred in 2021, more than two years ago. And this particular scheme, which plays off this real-world tax event, has been around since then. But while the stimulus payments ended long ago, the related scheme has

evolved and changed as scam artists look for new ways to adjust their message to trick people.

Taxpayers should not be fooled by this message for many reasons. For example, these emails are routinely riddled with spelling errors and factual inaccuracies, like this example.

> "Dear Tax Payer, We hope this message finds you well. We are writing to inform you abount an important matter regarding your recent tax return filing. Our record indicate that we have received your tax return for the fiscal inconsistencies or missing information that require your attention and clarification. You will receive a tax refund of $976.00 , We will process this amount once you have submitted the document we need for the steps to claim your tax refund.
>
> Sender : INTERNAL REVENUE SERVICE"

Like many scams, this email urges people to click on a link so they can complete their "application." Instead, it takes the taxpayer to a website where identity thieves will try to harvest valuable personal information.

The misleading "You may be eligible for the ERC" claim. The IRS has observed a significant increase in false Employee Retention Credit (ERC) claims. The ERC, sometimes also called the Employee Retention Tax Credit or ERTC, is a pandemic-related credit for which only select employers qualify.

Scam promoters are luring people to improperly claim the ERC with "offers" online, in social media, on the radio, or through unsolicited phone calls, emails and even mailings that look like official government letters but have fake agency names and usually urge immediate action. These unscrupulous promoters make false claims about their company's legitimacy and often do not discuss some key eligibility factors, limitations and income tax implications that affect an employer's tax return. It's important to watch for warning signs such as promoters who say they can quickly determine someone's eligibility without details, and those who charge up-front fees or a fee based on a percentage of the ERC claimed.

Anyone who improperly claims the ERC must pay it back, possibly with penalties and interest.

Eligible employers who need help claiming the ERC should work with a trusted tax professional. False ERC claims were so widespread this year that the IRS added them to its annual Dirty Dozen list of tax scams.

The "Claim your tax refund online" scheme. Identity thieves know that the concept of free or overlooked money is tempting for people. So the IRS routinely sees email and text schemes playing off tax refunds and suggesting people have somehow missed getting their tax refund.

A variation hitting inboxes in recent weeks has a blue headline proclaiming people should "Claim your tax refund online."

Again, there are telltale warning signs, including misspellings and urging people to click a link for help to "claim tax refund." Here's one example.

> "We cheked an error in the calculation of your tax from the last payment, amounting to $ 927,22. In order for us to return the excess payment, you need to create a E-Refund after which the funds will be credited to your specified bank. Please click below to claim your tax refund. If we are unable to complete within 3 days, all pending will be cancelled."

The "Help You Fix-It" text scheme. In another text scam seen in recent weeks, identity thieves come up with a name on a text message that tries to sound official, like "govirs-accnnt2023." They then send a variety of messages that say there's a problem with a person's tax return but, not to worry, the anonymous sender of the text message can help resolve the problem if they click on a link.

Like others, there are many red flags on these text messages, including misspellings and factual inaccuracies:

> "MSG … IRS:You federal return was ban-by the IRS. Don't worry, we'll help you fix it. Click this link."

The "Delivery Service" scam at your door. Earlier this month, the IRS warned 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 that arrives 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."

Receive a scam message? People that receive these scams by email should send the email to phishing@irs.gov. People can forward the message, but IRS cybersecurity experts prefer to see the full email header to help them identify the scheme.

If people are victims after clicking and entering their information, they should report the email to phishing@irs.gov – but they should also file a complaint with Treasury Inspector General for Tax Administration and visit IdentityTheft.gov and Identity Theft Central.

More 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 from scammers posing as legitimate organizations in the tax and financial community, including the IRS and the 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.

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.