THE TAXBOOK News
Release Date: 3/23/23

IRS Warns Taxpayers About New Email and Text Message Scams

Cross References

- IR-2023-51, March 21, 2023

Email and text scammers frequently use tax season as a way of tricking people into giving out personal information that can be used to steal a taxpayer's identity.

"With people anxious to receive the latest information about a refund or other tax issue, scammers will regularly pose as the IRS, a state tax agency or others in the tax industry in emails and texts. People should be incredibly wary about unexpected messages like this that can be a trap, especially during filing season," said IRS Commissioner Danny Werfel.

Phish or smish: Avoid getting hooked by either. 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 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. There are two main types:

- Phishing is an email sent by fraudsters claiming to come from the IRS or another legitimate organization, including state tax organizations or a financial firm. The email lures the victims into the scam by a variety of ruses such as enticing victims with a phony tax refund or frightening them with false legal/criminal charges for tax fraud.
- Smishing is a text or smartphone SMS message that uses the same technique as phishing. Scammers often use alarming language like, "Your account has now been put on hold," or "Unusual Activity Report" with a bogus "Solutions" link to restore the recipient's account. Unexpected tax refunds are another potential target for scam artists.

The IRS initiates most contacts through regular mail and will never initiate contact with taxpayers by email, text or social media regarding a bill or tax refund.

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.