Security Summit warns of new IRS impersonation email scam; reminds taxpayers the IRS does not send unsolicited emails

IR-2019-145, August 22, 2019

WASHINGTON — The Internal Revenue Service and its Security Summit partners today warned taxpayers and tax professionals about a new IRS impersonation scam campaign spreading nationally on email. Remember: the IRS does not send unsolicited emails and never emails taxpayers about the status of refunds.

The IRS this week detected this new scam as taxpayers began notifying phishing@irs.gov about unsolicited emails from IRS imposters. The email subject line may vary, but recent examples use the phrase "Automatic Income Tax Reminder" or "Electronic Tax Return Reminder."

The emails have links that show an IRS.gov-like website with details pretending to be about the taxpayer's refund, electronic return or tax account. The emails contain a "temporary password" or "one-time password" to "access" the files to submit the refund. But when taxpayers try to access these, it turns out to be a malicious file.

"The IRS does not send emails about your tax refund or sensitive financial information," said IRS Commissioner Chuck Rettig. "This latest scheme is yet another reminder that tax scams are a year-round business for thieves. We urge you to be on-guard at all times."

This new scam uses dozens of compromised websites and web addresses that pose as IRS.gov, making it a challenge to shut down. By infecting computers with malware, these imposters may gain control of the taxpayer's computer or secretly download software that tracks every keystroke, eventually giving them passwords to sensitive accounts, such as financial accounts.

The IRS, state tax agencies and the tax industry, which work together in the Security Summit effort, have made progress in their efforts to fight stolen identity refund fraud. But people remain vulnerable to scams by IRS imposters sending fake emails or harrassing phone calls.

The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information. This includes requests for PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts.

The IRS also doesn't call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes. See Report Phishing and Online Scams for more details.

Page Last Reviewed or Updated: 22-Aug-2019