IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS, Summit partners issue urgent EFIN scam alert to tax professionals

IR-2021-34, Feb. 10, 2021

WASHINGTON – The Internal Revenue Service, state tax agencies and tax industry today warned tax professionals of a new scam email that impersonates the IRS and attempts to steal Electronic Filing Identification Numbers (EFINs).

The Security Summit partners said the latest scheme, arriving just before the start of the nation's tax season, should serve as another reminder that tax professionals remain prime targets for identity thieves. These thieves try to steal client data and tax preparers' identities that will allow them to file fraudulent tax returns for refunds.

"Phishing scams are the most common tool used by identity thieves to trick tax professionals into disclosing sensitive information, and we often see increased activity during filing season," said IRS Commissioner Chuck Rettig. "Tax professionals must remain vigilant. The scammers are very active and very creative."

The latest scam email says it is from "IRS Tax E-Filing" and carries the subject line "Verifying your EFIN before e-filing."

The IRS warns tax pros not to take any of the steps outlined in the email, especially responding to the email. The body of the bogus email states:

In order to help protect both you and your clients from unauthorized/fraudulent activities, the IRS requires that you verify all authorized e-file originators prior to transmitting returns through our system. That means we need your EFIN (e-file identification number) verification and Driver's license before you e-file.

Please have a current PDF copy or image of your EFIN acceptance letter (5880C Letter dated within the last 12 months) or a copy of your IRS EFIN Application Summary, found at your e-Services account at IRS.gov, and Front and Back of Driver's License emailed in order to complete the verification process. Email: (fake email address)

If your EFIN is not verified by our system, your ability to e-file will be disabled until you provide documentation showing your credentials are in good standing to e-file with the IRS.

Tax professionals who received the scam should save the email as a file and then send it as an attachment to phishing@irs.gov. They also should notify the Treasury Inspector General for Tax Administration at www.TIGTA.gov to report the IRS impersonation scam. Both TIGTA and the IRS Criminal Investigation division are aware of the scam.

Like all phishing email scams, it attempts to bait the receiver to take action (opening a link or attachment) with a consequence for failing to do so (disabling the account). The links or attachment may be set up to steal information or to download malware onto the tax professional's computer.

In this case, the tax preparers are being asked to email documents that would disclose their identities and EFINs to the thieves. The thieves can use this information to file fraudulent returns by impersonating the tax professional.

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Tax professionals also should be aware of other common phishing scams that seek EFINs, Preparer Tax Identification Numbers (PTINs) or e-Services usernames and passwords.

Some thieves also pose as potential clients, an especially effective scam currently because there are so many remote transactions during the pandemic. The thief may interact repeatedly with a tax professional and then send an email with an attachment that claims to be their tax information.

The attachment may contain malware that allows the thief to track keystrokes and eventually steal all passwords or take over control of the computer systems.

Some phishing scams are ransomware schemes in which the thief gains control of the tax professionals' computer systems and holds the data hostage until a ransom is paid. The Federal Bureau of Investigation (FBI) has warned against paying a ransom because thieves often leave the data encrypted.

For additional information and help, tax professionals should review Publication 4557, Safeguarding Taxpayer Data, and Identity Theft Information for Tax Professionals.

-30-