ADV 2021-03
SECURITY SUMMIT

ADVISORY FOR TAX PROFESSIONALS
FEBRUARY 11, 2021

# Security Summit warns tax professionals about new email scam

*Criminals impersonate IRS to try to steal tax preparers' electronic filing ID numbers*

PROVIDENCE — The Rhode Island Division of Taxation, the Internal Revenue Service, and other members of the Security Summit warn tax professionals about 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 official start of the tax-filing 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 and use that information 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," he said.

"We urge tax professionals to take every possible precaution throughout this filing season to safeguard their information and their clients' information," said Rhode Island Tax Administrator Neena Savage.

## Details about latest scam

The latest scam email claims to be from "IRS Tax E-Filing" and carries the following subject line: "Verifying your EFIN before e-filing."

The Security Summit warns tax professionals not to take any of the steps outlined in the email, and urges tax professionals not to respond to the email. The body of the bogus email reads as follows:

> *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:* (a fake email address is inserted here by the criminal)

*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.*


*2800 E. Commerce Center Place, Tucson, AZ 85706*

Tax professionals who received the scam email described above should save the email as a file and then send it as an attachment to the following email address: phishing@irs.gov. Tax professionals 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.

### Don't take the bait

Like all phishing email scams, this one 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.

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.

### Criminals posing as clients

Some thieves also pose as potential clients, an especially effective scam currently because there are so many remote transactions during the coronavirus (COVID-19) 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.

**About the Security Summit**

The Security Summit consists of the IRS, state tax agencies, and the tax community -- including tax preparation firms, software developers, processors of payroll and tax financial products, tax professional organizations, and financial institutions.

Partners in the Security Summit work together to combat identity theft and fight other scams to protect the nation's taxpayers.

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") through this link: https://www.irs.gov/pub/irs-pdf/p4557.pdf.

Tax professionals also should read the information available on an IRS webpage that focuses on identity theft information for tax professionals: https://www.irs.gov/identity-theft-fraud-scams/identity-theft-information-for-tax-professionals

*The Rhode Island Division of Taxation office is open to the public 8:30 a.m. to 3:30 p.m. business days. To learn more, see the agency's website: www.tax.ri.gov.*