Rhode Island Department of Revenue
Division of Taxation

ADV 2018-01
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JANUARY 9, 2018

Security Summit warns tax professionals about fraud

Early signs indicate that cybercriminals are already at work as filing season approaches

PROVIDENCE, R.I. – Cybercriminals are already at work as the nation's tax season approaches, according to the Rhode Island Division of Taxation, the Internal Revenue Service, and other members of the Security Summit.

Criminals are using a new round of emails posing as potential clients or even the IRS to trick tax practitioners into disclosing sensitive information, the Security Summit warned tax professionals today.

The Security Summit partners encourage tax practitioners to be wary of communicating solely by email with potential or even existing clients, especially if unusual requests are made.

Data breach thefts have given thieves millions of identity data points including names, addresses, Social Security numbers, and email addresses. If in doubt, tax practitioners should call to confirm a client's identity.

"Numerous data breaches last year mean the entire tax preparation community must be on high alert this filing season to any unusual activity. Thieves may try to leverage stolen identities to steal even more data that will allow them to better impersonate taxpayers and file fraudulent tax returns for refunds," said Rhode Island Tax Administrator Neena Savage.

The IRS, state tax agencies, and the tax industry, acting as the Security Summit, have made significant strides in fighting identity theft. But cybercriminals continue to evolve and Summit partners need the help of everyone, including tax professionals and taxpayers, to continue this progress.

RECENT SCHEMES

In recent days, tax professionals have reported numerous attempts by criminals to pierce their security by posing as potential clients. Crooks are using the same tactic they did last year (IR-2017-03), using phishing emails to trick tax practitioners into opening a link or attached document.

The criminals, posing as potential clients, send initial emails to tax practitioners. In recent days, the IRS has seen the following early variations of these email schemes:

- *"Happy new year to you and yours. I want you to help us file our tax return this year as our previous CPA/account passed away in October. How much will this cost us?...hope to hear from you soon."*
- *"Please kindly look into this issue, A friend of mine introduced you to me, regarding the job you did for him on his 2017 tax. I tried to reach you by phone earlier today but it was not connecting, attach is my information needed for my tax to be filed if you need any more Details please feel free to contact me as soon as possible and also send me your direct Tel-number to rich (sic) you on."*
- *"I got your details from the directory. I would like you to help me process my tax. Please get back to me asap so I can forward my details."*

If the tax practitioner responds, the cybercriminal will send a second email that contains either a phishing URL or an attached document that contains a phishing URL, claiming their tax data is enclosed. The criminal wants the tax pro to click on the link or attachment and then enter their credentials. In some cases, the URL or attachment might be malicious and if clicked will download malicious software onto the tax pro's computer.

Depending on the malware involved, this scheme could give criminals access to the tax practitioners' secure accounts or sensitive data. It may even give the cybercriminal remote control of the tax professionals' computers.

The IRS also has received recent reports of criminals again posing as IRS e-Services, asking tax pros to sign into their accounts and providing a disguised link. The link, however, sends tax pros to a fake e-Services site that steals their usernames and passwords.

This type of scam is one of the reasons the IRS has moved e-Services to the more secure identity-proofing process called Secure Access. It is important that all e-Services account holders upgrade their accounts to this more rigorous authentication process. E-Services account holders who have not updated their accounts should do so immediately. See Important Update about Your e-Services Account.

Tax practitioners receiving emails from criminals posing as the IRS, the Rhode Island Division of Taxation, or their tax software provider, should go directly to the main website, such as IRS.gov, or www.tax.ri.gov, rather than opening any links or attachments. Forward attempted phishing emails to phishing@irs.gov. Remember, neither the IRS nor the Rhode Island Division of Taxation sends unsolicited emails.

The Rhode Island Division of Taxation office is at One Capitol Hill in Providence, R.I., diagonally across from the Smith Street entrance to the State House, and 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, or call (401) 574-8829.