Rhode Island Department of Revenue
Division of Taxation

ADV 2018-31
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 31, 2018

Tax professionals urged to beware of spear-phishing email

Data thieves use it to enter practitioner's digital network, steal client information

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit urge tax professionals to beware of spear-phishing email. Use of such email is the most common method that data thieves use to enter a practitioner's digital networks and steal client information.

Tax professionals who fall victim to spear-phishing tactics voluntarily disclose sensitive password information or voluntarily download malicious software, enabling thieves to breach their security systems. The Security Summit reminds tax professionals that they themselves must be the first line of defense in protecting client data.

The Security Summit is a partnership formed by the IRS, the Rhode Island Division of Taxation, other states' tax agencies, and the private-sector tax community to combat tax-related identity theft.

Although the Summit is making progress, cybercriminals continue to evolve, and data thefts at tax professionals' offices are on the rise. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder to detect.

Spear-phishing emails differ from general phishing emails in that the thief has researched his target before sending an email. An email may appear to be from a colleague, a client, a cloud storage provider, tax software provider, or even the IRS or the states.

The objective of a spear-phishing email is to pose as a trusted source and bait the recipient into opening an embedded link or an attachment. The email may make an urgent plea to update an account immediately. A link may seem to go to another trusted website, for example a cloud storage or tax software provider login page, but it's actually a website controlled by the thief.

An attachment may contain malicious software called keylogging that secretly infects computers and provides the

This is the fourth in a series of Security Summit announcements called "Protect Your Clients; Protect Yourself: Tax Security 101."

The Security Summit awareness campaign is intended to provide tax professionals with the basic information they need to better protect taxpayer data and to help prevent the filing of fraudulent tax returns.

thief with the ability to see every keystroke. Thieves can steal passwords to various accounts or even take remote control of computers, enabling them to steal taxpayer data.

For those who fall for a spear-phishing scam and ultimately allow a thief to access their email account, the criminal can use that access to create additional spear-phishing scams. The criminal does this by targeting those with whom the original user has exchanged emails, including clients, colleagues, and friends.

Tips for tax professionals to avoid phishing scams

Educated employees are the key to avoiding phishing scams, but these simple steps also can help protect against stolen data:

- Use separate personal and business email accounts; protect email accounts with strong passwords and two-factor authentication if available.
- Install an anti-phishing tool bar to help identify known phishing sites. Anti-phishing tools may be included in security software products.
- Use security software to help protect systems from malware and scan emails for viruses.
- Never open or download attachments from unknown senders, including potential clients; make contact first by phone, for example.
- Send only password-protected and encrypted documents if files must be shared with clients via email.
- Do not respond to suspicious or unknown emails; if IRS-related, forward to phishing@irs.gov.

In addition to these steps, the Security Summit reminds all professional tax preparers that they must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule.

Tax professionals can get help with security recommendations by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security: the Fundamentals by the National Institute of Standards and Technology. In addition, Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation of data theft information available on IRS.gov.

The Rhode Island Division of Taxation office is at One Capitol Hill in Providence, R.I., diagonally across from the Smith Street entrance of 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 Division's website: www.tax.ri.gov.