ADV 2019-17
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 31, 2019

Security Summit urges tax professionals to beware of phishing emails

Cybercriminals use this common tactic to steal sensitive taxpayer data

PROVIDENCE — The Internal Revenue Service, the Rhode Island Division of Taxation, and other members of the Security Summit urge tax professionals to beware of the continuing threat of phishing emails, which remain the most common tactic used by cybercriminals to steal sensitive data.

"You can take all the cybersecurity steps in the world, but tax professionals and others in the business world should remember you are only as safe as your least educated employee," said Chuck Rettig, IRS Commissioner. "Cybercriminals use phishing emails and malware to gain control of computer systems or to steal usernames and passwords. These can provide a treasure trove of information that can lead to tax-related identity theft."

Although the Security Summit has made major progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices continue to be seen across the nation. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder for the Security Summit partners to detect, said Rhode Island Tax Administrator Neena S. Savage.

Educate yourself on phishing emails

More than 90% of all data thefts start with a phishing email. The employee may open a link that takes them to a fake site or open an attachment that is embedded with malware that secretly downloads onto their computers.

The Security Summit often sees tax professionals victimized after being targeted with a tactic called spear phishing. 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 the tax pro 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, which secretly infects computers and provides the 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.

Common spear-phishing scams seen by the Security Summit include thieves posing as prospective clients, sending unsolicited emails to tax professionals. After an exchange of emails, the thief sends

an email with an attachment, claiming it contains the tax information needed to prepare a return. Instead, it contains spyware that allows thieves to track each keystroke.

The Security Summit also sees thieves posing as tax software providers or data storage providers with emails containing links that go to web pages that mirror real sites. The thieves' goal is to trick tax professionals into entering their usernames and passwords into these fake sites, which the crooks then steal.

Another trick used by thieves is rather than stealing the data, they encrypt it, a practice known as ransomware. Once they encrypt the data, thieves demand a ransom in return for the code to unencrypt the data. The Federal Bureau of Investigation warns users not to pay the ransom because thieves often do not provide the code. The FBI has called ransomware attacks a growing threat to businesses and others.

Educated employees are the key to avoiding phishing scams, and office systems are only as safe as the least informed employee. The following 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.

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.

ADDITIONAL RESOURCES: The Security Summit reminds all tax professionals that they must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. Get help with security recommendations by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data (PDF), and Small Business Information Security: the Fundamentals (PDF) by the National Institute of Standards and Technology.

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 agency's website: www.tax.ri.gov.