Rhode Island Department of Revenue
Division of Taxation

ADV 2017-43
TAX ADMINISTRATION

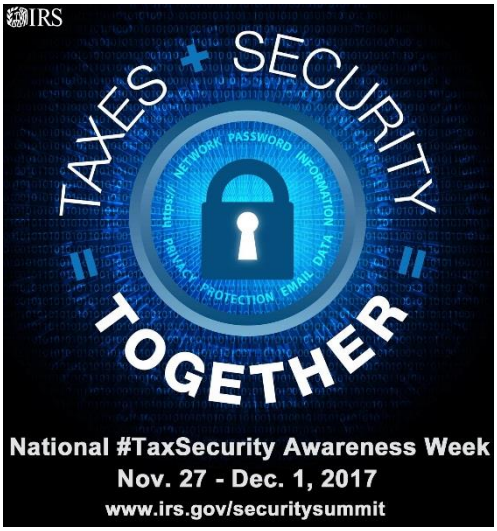
ADVISORY FOR TAX PROFESSIONALS
NOVEMBER 30, 2017

W-2 email scam threatens information held by employers

Tips for taxpayers, businesses, and tax professionals from the Security Summit

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit warn the nation's business, payroll, and human resource communities about a growing W-2 email scam that threatens sensitive tax information held by employers.

These emails may start with a simple, "Hey, you in today?" and, by the end of the exchange, all of an organization's Forms W-2 for their employees may be in the hands of cybercriminals. This puts workers at risk for tax-related identity theft.



The W-2 scam has emerged as one of the most dangerous and successful phishing attacks: Hundreds of employers and tens of thousands of employees fell victim to the scheme in the past year. This scam is such a threat to taxpayers that a special IRS reporting process has been established.

The IRS, state tax agencies, and the tax community -- partners in the Security Summit -- are marking "National Tax Security Awareness Week" with a series of reminders to taxpayers and tax professionals. Today's topic is the W-2 scam.

INCOME AND WITHHOLDING INFORMATION

Because the Security Summit partners have successfully made inroads into stopping stolen identity refund fraud, criminals now need more information to file a fraudulent return. That means they need more accurate data about taxpayers, causing them to target tax practitioners, payroll professionals, and employers. The Form W-2 contains income and withholding information necessary to file a tax return.

All employers are at risk. In 2017, the W-2 scam made victims of businesses large and small, public schools and universities, as well as tribal governments, charities, and hospitals. The scam, which grows larger each year, will likely make the rounds again in 2018.

The Security Summit warns employers – in the public sector and in the private sector – to beware of this scheme and to educate employees, especially those in human resources and payroll departments who are often the first targets.

Following is an example of a business email compromise, or business email spoofing, in which the thief poses as a company executive, school official, or someone of authority within the organization:

The crook will send an email to one employee with payroll access, requesting a list of all employees and their Forms W-2. The thief may even specify the format in which he or she wants the information. The subject line has hundreds of variations along the lines of "review", "manual review", or "request."

Because payroll officials believe they are corresponding with an executive, it may take weeks for someone to realize a data theft has occurred. Generally, the criminals are trying to quickly take advantage of their theft, sometimes filing fraudulent tax returns within a day or two.

Because of the W-2 scam's threat to tax administration for both federal and state governments, a special reporting process has been established to quickly alert the IRS and state tax agencies. Detailed reporting steps may be found at Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers.

FOLLOWING IS AN ABBREVIATED LIST OF HOW TO REPORT THESE SCHEMES:

- Email dataloss@irs.gov to notify the IRS of a W-2 data loss and provide contact information. In the subject line, type "W2 Data Loss" so that the email can be routed properly. Do not attach any employee personally identifiable information data.
- Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.
- Businesses/payroll service providers should file a complaint with the FBI's Internet Crime Complaint Center (IC3.gov). Businesses/payroll service providers may be asked to file a report with their local law enforcement agency.
- Notify employees so they may take steps to protect themselves from identity theft. The Federal Trade Commission's www.identitytheft.gov provides guidance on general steps employees should take.
- Forward the scam email to phishing@irs.gov.

Employers are urged to put steps and protocols in place for the sharing of sensitive employee information such as Forms W-2. One example would be to have two people review any distribution of sensitive W-2 data or wire transfers. Another example would be to require a verbal confirmation before emailing W-2 data. Employers also are urged to educate their payroll or human resources departments about these scams.

As part of the Security Summit effort, the IRS, state tax agencies, and the tax industry are working together to fight against tax-related identity theft and to protect taxpayers. Everyone can help. Be alert and guard against the W-2 scam.

Taxpayers are also encouraged to visit the "Taxes. Security. Together." awareness campaign, or review IRS Publication 4524, Security Awareness for Taxpayers, to learn more.

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.