Rhode Island Department of Revenue
Division of Taxation

ADV 2018-05
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JANUARY 17, 2018

Security Summit warns employers about W-2 scam

Cybercriminals trick personnel into disclosing confidential taxpayer information

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, the Internal Revenue Service, tax agencies from other states, and the tax industry today urged all employers to educate their payroll personnel about a Form W-2 phishing scam that made victims of hundreds of organizations and thousands of employees last year.

The Form W-2 scam has emerged as one of the most dangerous phishing emails in the tax community. During the last two tax seasons, cybercriminals tricked payroll personnel or people with access to payroll information into disclosing sensitive information for entire workforces.

The scam affected all types of employers, from small and large businesses to public schools and universities, hospitals, tribal governments, and charities.

Reports to phishing@irs.gov from victims and non-victims about this scam jumped to approximately 900 in 2017, compared to slightly over 100 in 2016.

Last year, more than 200 employers were victimized, which translated into hundreds of thousands of employees who had their identities compromised.

By alerting employers now, the IRS, the Rhode Island Division of Taxation, and other partners in the Security Summit hope to limit the effect of this scam in 2018.

The IRS last year also created a new process by which employers should report these scams (see next page). There are steps the IRS can take to protect employees, but only if the agency is notified immediately by employers about the theft.

HOW THE SCAM WORKS

Here's how the scam works: Cybercriminals do their homework, identifying chief operating officers, school executives, or others in positions of authority. Using a technique known as business email compromise (BEC) or business email spoofing (BES), criminals posing as executives send emails to payroll personnel requesting copies of Forms W-2 for all employees.

The Form W-2 contains the employee's name, address, Social Security number, income, and withholdings. Criminals use that information to file fraudulent tax returns, or the criminals post that information for sale on the Dark Net.

The initial email may be a friendly, "hi, are you working today" exchange before the criminal asks for all Form W-2 information. In several reported cases, after the criminals acquired the workforce information, they immediately followed that up with a request for a wire transfer.

The IRS, the Division of Taxation, and other Security Summit partners seek to educate payroll or finance personnel about the scam. The Security Summit partners also urge employers to consider creating a policy to limit the number of employees who have authority to handle Form W-2 requests and that they require additional verification procedures to validate the actual request before emailing sensitive data such as employee Form W-2s.

If the business or organization victimized by these attacks notifies the IRS, the IRS can take steps to help prevent employees from being victims of tax-related identity theft. However, because of the nature of these scams, some businesses and organizations did not realize for days, weeks or months that they had been scammed.

HOW TO REPORT W-2 DATA THEFTS

The IRS established a special email notification address specifically for employers to report Form W-2 data thefts. Here's how Form W-2 scam victims can notify the IRS: Email dataloss@irs.gov to notify the IRS of a Form W-2 data loss. In the subject line of the email, type "W2 Data Loss" so that the email can be routed properly. Do not attach any information or data which could personally identify an employee. In the email, include the following:

- Business name
- Business employer identification number (EIN) associated with the data loss
- Contact name
- Contact phone number
- Summary of how the data loss occurred
- Volume of employees impacted

Businesses and organizations that fall victim to the scam, and organizations that only receive a suspect email but do not fall victim to the scam, should send the full email headers to phishing@irs.gov and use "W2 Scam" in the subject line.

Employers can learn more at: Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers. Employers should be aware that cybercriminals' scams constantly evolve. Finance and payroll personnel should be alert to any unusual requests for employee data.

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, or call (401) 574-8829.