IRS Warns of Tax Scam with Fake W-2 Forms

ISAAC M. O'BANNON, MANAGING EDITOR ON JAN 17, 2018

U.S. businesses need to watch out for a Form W-2 phishing scam that made victims of hundreds of organizations and thousands of employees last year.

The IRS says 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 nonvictims 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 and its partners in the Security Summit effort hope to limit the success of this scam in 2018. The IRS last year also created a new process by which employers should report these scams. There are steps the IRS can take to protect employees, but only if the agency is notified immediately by employers about the theft.

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), fraudsters 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 they post it for sale on the Dark Net.

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

In addition to educating payroll or finance personnel, the IRS and 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.