PRESS RELEASE

Internal Revenue Service - Criminal Investigation
Boston Field Office
Special Agent in Charge Joel P. Garland

Date: March 7, 2017

Contact: SA Amy L. Hosney, PIO
IRS – Criminal Investigation
(203) 492-8774
amy.hosney@ci.irs.gov
CI Release #: BOSFO-2017-01

Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others

Connecticut & Massachusetts **—** The Internal Revenue Service, state tax agencies and the tax industry issued an urgent alert in early February to all employers that the Form W-2 email phishing scam has evolved beyond the corporate world and is spreading to other sectors, including school districts, tribal organizations and nonprofits.

IRS Special Agent in Charge Joel P. Garland leads IRS Criminal Investigation in the six New England states. "We are seeing a surge in W-2 phishing scams in New England, especially Connecticut and Massachusetts", said Garland today. "Thousands of employees have been impacted by these email scams, whereby Personally Identifiable Information (PII) and wage data are unwittingly turned over to fraudsters with malicious intent. IRS-CI will continue to vigorously investigate these crimes and assist taxpayers who become victims of stolen identity refund fraud."

In a related development, the W-2 scammers are coupling their efforts to steal employee W-2 information with an older scheme on wire transfers that is victimizing some organizations twice.

"This is one of the most dangerous email phishing scams we've seen in a long time. It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone's help to turn the tide against this scheme,'' said IRS Commissioner John Koskinen.

When employers report W-2 thefts immediately to the IRS, the agency can take steps to help protect employees from tax-related identity theft. The IRS, state tax agencies and the tax industry, working together as the Security Summit, have enacted numerous safeguards in 2016 and 2017 to identify fraudulent returns filed through scams like this. As the Summit partners make progress, cybercriminals need more data to mimic real tax returns.

Here's how the scam works: Cybercriminals use various spoofing techniques to disguise an email to make it appear as if it is from an organization executive. The email is sent to an employee in the payroll or human resources departments, requesting a list of all employees and their Forms W-2. This scam is sometimes referred to as business email compromise (BEC) or business email spoofing (BES).

The Security Summit partners urge all employers to be vigilant. The W-2 scam, which first appeared last year, is circulating earlier in the tax season and to a broader cross-section of

organizations, including school districts, tribal casinos, chain restaurants, temporary staffing agencies, healthcare and shipping and freight. Those businesses that received the scam email last year also are reportedly receiving it again this year.

Security Summit partners warned of this scam's reappearance last week but have seen an upswing in reports in recent days.

New Twist to W-2 Scam: Companies Also Being Asked to Wire Money
In the latest twist, the cybercriminal follows up with an "executive" email to the payroll or comptroller and asks that a wire transfer also be made to a certain account. Although not tax related, the wire transfer scam is being coupled with the W-2 scam email, and some companies have lost both employees' W-2s and thousands of dollars due to wire transfers.

The IRS, states and tax industry urge all employers to share information with their payroll, finance and human resources employees about this W-2 and wire transfer scam. Employers should consider creating an internal policy, if one is lacking, on the distribution of employee W-2 information and conducting wire transfers.

Steps Employers Can Take If They See the W-2 Scam

Organizations receiving a W-2 scam email should forward it to phishing@irs.gov and place "W2 Scam" in the subject line. Organizations that receive the scams or fall victim to them should file a complaint with the Internet Crime Complaint Center (IC3,) operated by the Federal Bureau of Investigation.

Employees whose Forms W-2 have been stolen should review the recommended actions by the Federal Trade Commission at www.identitytheft.gov or the IRS at www.irs.gov/identitytheft. Employees should file a Form 14039, Identity Theft Affidavit, if the employee's own tax return rejects because of a duplicate Social Security number or if instructed to do so by the IRS.

The W-2 scam is just one of several new variations that have appeared in the past year that focus on the large-scale thefts of sensitive tax information from tax preparers, businesses and payroll companies. Individual taxpayers also can be targets of phishing scams, but cybercriminals seem to have evolved their tactics to focus on mass data thefts.

Be Safe Online

In addition to avoiding email scams during the tax season, taxpayers and tax preparers should be leery of using search engines to find technical help with taxes or tax software. Selecting the wrong "tech support" link could lead to a loss of data or an infected computer. Also, software "tech support" will not call users randomly. This is a scam.

Taxpayers searching for a paid tax professional for tax help can use the IRS Choosing a Tax Professional lookup tool or if taxpayers need free help can review the Free Tax Return Preparation Programs. Taxpayers searching for tax software can use Free File, which offers 12 brand-name products for free, at www.irs.gov/freefile. Taxpayer or tax preparers looking for tech support for their software products should go directly to the provider's web page.

Tax professionals also should beware of ongoing scams related to IRS e-Services. Thieves are trying to use IRS efforts to make e-Services more secure to send emails asking e-Services users to update their accounts. Their objective is to steal e-Services users' credentials to access these important services.

See also:
- Affected employers and companies should also alert the state tax agencies by notifying StateAlert@taxadmin.org.

###