CLIENT ALERTS & INSIGHTS

Gone Phishing: IRS Warns Businesses of Tax Season W-2 Phishing Scam

FEBRUARY 10, 2017

Authors: Alison K. Evans

Tax season is upon us, and as millions of people nationwide are preparing to file their tax returns, the Internal Revenue Services (IRS) has issued an urgent warning regarding a recurring e-mail phishing scheme targeting businesses. For the non-techie, phishing occurs when an internet fraudster impersonates a business to trick consumers into giving out their personal information.

“This is one of the most dangerous email phishing scams we’ve seen in a long time,” said IRS Commissioner John Koskinen. “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.”

According to the IRS, the fraudster will send an email to payroll and/or human resources professionals that appears to be a legitimate email from company executives and requests personal information about company employees, including their Forms W-2. The emails, which commonly include the actual name of the company chief executive officer, often include requests, such as:

- “Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review.”
- “Can you send me the updated list of employees with full details (Name, Social Security Number, Date of Birth, Home Address, Salary).”
- “I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me ASAP.”

The fraudsters then either sell the information obtained or use it to file fraudulent tax returns and obtain refunds in the name of unsuspecting employees. Fraudsters may even follow up with a second “executive” request for the personnel to transfer funds by wire to a bank account to cover payroll or other of the company’s bills, thus obtaining not only unauthorized access to employees’ W-2 information, but also scamming companies out of thousands of dollars.

I am an employee, and I think I just received a phishing email. What do I do?

The best advice for employees is to remain vigilant. “If your CEO appears to be emailing you for a list of company employees, check it out before your respond,” suggests the IRS Commissioner. “Everyone has a responsibility to remain diligent about confirming the identify of people requesting personal information about employees.”

If you do receive a suspicious phishing email, report it to the IRS by forwarding the correspondence to phishing@irs.gov with "W-2 Scam" in the subject line. In addition, companies can file complaints with the Internet Crime Complaint Center (IC3), operated by the FBI, and alert state tax agencies by notifying StateAlert@taxadmin.org.

My employer just informed me that my W-2 information was disclosed to an email phisher. What can I do to protect myself from tax return fraud and identity theft?

Individual employees who have been informed that their W-2 information was disclosed to a scammer can take a number of steps to protect their personal information and prevent identity theft, such as reviewing the recommendations of the Federal Trade Commission at www.identitytheft.gov and the IRS at www.irs.gov/identitytheft. The IRS also advises individuals to file a Form 14039 Identity Theft Affidavit with the IRS if the individual's own tax return is rejected because of a duplicate Social Security Number.

Of course, individuals can avoid tax return fraud entirely by filing their returns early, before the fraudsters can.

I am a CEO, and I am concerned my business may fall victim to this phishing scam. What do you recommend to help protect my employees?

To counter internet scam artists and fraudsters, and to prevent or mitigate potential security incidents, companies should put in place a comprehensive data privacy and security program that includes a robust training component. Training is key for companies who wish to avoid falling victim to W-2 phishing scams and other data privacy and security scams. Such training, should remind employees of the following:

- Email is not a secure method of transmitting personal or financial information, so do not email such information.
- Be cautious about opening attachments and downloading files form emails, regardless of who sent them - - these files can contain viruses or other malware that weaken your company's computer security system.
- Delete emails and text messages that ask to confirm or provide personal information (i.e., credit card and bank account numbers, Social Security numbers, passwords, etc.) - - legitimate companies do not ask for this information in an email or text.
- Do not reply, and do not click on email links, texts, pop-up messages or call phone numbers that ask for your personal or financial information - - these message generally direct you to spoof sites that look real but whose purpose is to steal your information.

For more information, please contact Joseph P. Yonadi, Jr., Partner, Benesch, Friedlander, Coplan & Aronoff LLP, at jyonadi@beneschlaw.com or at 216.363.449, or Alison K. Evans, Associate, at aevans@beneschlaw.com or at 216.363.4168.