PHISHING SEASON OPENS FOR 2016 TAX FILINGS – BEWARE OF “W-2 PHISHING SCAMS”

Date: 11 April 2016

Labor, Employment and Workplace Safety Alert

By: David A. Bateman, Bridget A. Blinn-Spears

Tax season brings many headaches, but none as miserable as sophisticated scammer efforts to steal employee W-2 information. Using social engineering and modest technological tools, a "spear phishing" attack seeks to trick unsuspecting human resources (HR) personnel into revealing employee W-2 records. Armed with that information, the scammers quickly file for the employees' tax refunds.

The Internal Revenue Service (IRS) estimates that it paid over $31 billion in fraudulent refunds in 2015. Here are practical steps to help your company avoid becoming victimized during this "phishing season."

SIMPLE MISTAKE: ENORMOUS IMPACT

An HR intern receives an e-mail apparently from a company executive urgently requesting payroll information from the previous year. Eager to be responsive, the employee quickly replies with the information, which includes employees' names, social security numbers, addresses, and compensation information. A few days later, reports begin trickling into management that employees are receiving rejection emails from the IRS when they try to file their taxes—someone has already filed a return using their information. Other employees begin receiving letters from the IRS indicating the agency believes someone has attempted to file a fraudulent return with their information.

The company has state-of-the-art cybersecurity measures in place. It has no indication its systems have been breached. To its chagrin, it discovers the data breach came from human error: its eager-to-please intern's email responded to a simple, but sophisticated, phishing scheme, releasing highly confidential W-2 information to an untraceable IP address. The company wisely contacts outside counsel and learns that thousands of companies are falling prey to this same scheme across the country. The naïve intern's mistake could have wide-reaching consequences. The company must now navigate a complex maze of legal and ethical obligations while managing its distracted and upset workforce.

UPSURGE IN PHISHING ATTACKS AND NEW APPROACHES

The IRS recently issued an alert to HR and payroll professionals regarding a particular phishing scheme involving cybercriminals posing as CEOs and requesting information from their payroll departments. Despite this alert, and despite increased cybersecurity measures, companies continue to lose information as criminals manipulate the vulnerable link of their own personnel. The IRS noted the following language common to such emails this year:

"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 IRS has indicated a 400 percent surge in phishing and malware incidents in this tax season. This figure includes direct targeting of taxpayers through emails posing as IRS officials, tax software company employees, or other legitimate participants in the tax industry.

DO NOT TAKE THE BAIT: GET AHEAD OF THE PROBLEM!

Taking any or all of the following steps may help to fend off phishing attacks by increasing employee awareness and caution:

- Remind employees to treat all email requests for confidential information with suspicion, including those that appear at first blush to come from inside the company (including from top executives).
- Require employees take steps to avoid falling prey to phishing schemes:
  - Confirm any sensitive requests in person or with a phone call (to a number they obtain from the company directory, not from the email) to make sure they are genuine.
  - Avoid sending W-2 information and other data by email. Instead, walk it over and deliver it by hand.
  - Do not hit "Reply." Never send confidential or sensitive information in reply email. If you cannot avoid using email, draft a new email, double checking the correct address. Follow up to make sure it was received.
  - Use password protection on files containing confidential information. Communicate passwords in a separate email.
  - Be cautious opening attachments or downloading files from emails, particularly if they are unexpected.
  - Be particularly aware of spelling and grammatical errors or language that does not "sound like" a sender you know.
  - Use common sense. A short delay to double check an email's authenticity is well worth the time and effort.
- Coach supervisors and executives to encourage double checking and positively reinforce appropriate caution.

IF YOU ARE HOOKED: ACT SWIFTLY AND DELIBERATELY

Despite companies' best efforts, employees are human and systems are not failsafe. If an employee responds to a phishing scheme and releases confidential data regarding other employees, the particular circumstances of the breach will affect the proper course of action. The company's first steps should include:

- Determining basic information about how many employees are involved, where those employees are located, and whether the company is aware of any use of the stolen data.
- Involving the company's lawyers, whether they are in-house or outside counsel, to provide advice regarding next steps, which may include any or all of the following:
  - Who must be notified and what the notification must include;
  - Whether anyone else should be notified voluntarily;
  - Whether to provide required notices (or voluntary notices) directly or through a vendor;
  - Whether any insurance policy may provide some coverage;
  - Whether and how to provide credit monitoring or other identity theft protection for affected employees; and
  - Whether to craft appropriate communications to affected employees and, if needed, to the general public and/or the press.

DO NOT WAIT TO BE REELED IN: PREPARE PROACTIVELY

Quick and appropriate action is key to limiting or eliminating potential harm from wider use of stolen information targeting bank, credit card, phone, or utilities accounts or seeking to circumvent employment laws. The best course of action is staying ahead of phishing criminals by reminding employees to be cautious and implementing policies and practices to help safeguard information from employee error as well as computer attacks. As every sports fan knows, the best defense is a good offense.

KEY CONTACTS

DAVID A. BATEMAN
PARTNER
SEATTLE
+1.206.370.6682
DAVID.BATEMAN@KLGATES.COM

