Employers Take Note: Tax Season Phishing Scams on the Rise

Insights
2.20.18

It is tax season once again, and with it comes an increased threat of phishing scams targeting human resources and payroll personnel. In 2016, the IRS alerted employers to a then-emerging email phishing scheme in which messages purporting to come from company executives requested the release of personal information relating to employees, including W-2 tax forms. Since then, the scam has evolved into a significant threat facing employers in multiple industries, from small and large businesses to public schools and universities, hospitals, tribal governments and charities. According to the IRS, in 2017 alone, more than 200 employers reported falling victim to the scam, with hundreds of thousands of employees impacted.

The scam is set up by cybercriminals who research the identities of chief operating officers, or others in positions of authority, and then send "spoofing" emails to payroll or human resources personnel, posing as executives, and requesting copies of Forms W-2 for all employees. The emails use cloned company email addresses with authentic-looking company logos, colors, and signatures, in an effort to deceive the recipient into believing that the message is legitimate. The initial email is sometimes sent as a friendly introductory exchange, asking the employee if he/she is working today, before asking for the Form W-2 information.

If the unsuspecting recipients are deceived into thinking the emails are legitimate, they will comply with the request and end up delivering W-2 forms to the scam artists. These forms contain a treasure trove of employee personal data, including employees' names, addresses, social security numbers, income, and withholdings. Once the W-2 forms are received, the successful hackers often use the information to file fraudulent tax returns, or they post the information for sale on the Dark Net. If successful with the initial email, the cybercriminals sometimes follow up with a request for a fraudulent wire transfer as well.

To avoid falling victim to this scheme, employers should immediately warn employees about the risks associated with this scam. The notice and appropriate training should be given to payroll, human resources, and any other group of employees with access to personal identifiable information to be on the lookout for these phishing attempts or other red flags, such as requests for information not typically requested, or requests from individuals with whom the employees do not typically directly communicate. Employers should also take steps to limit the number of employees who have authority to access and disclose such information, and to implement procedures requiring

validation of any request for sensitive personal data, such as Form W-2s, as well as any requests for wire transfers.

Employers who have fallen victim to this scam may be subject to data breach notification requirements. These obligations can vary from state to state, and employers should consult their counsel to identify applicable notification requirements.

Additionally, employers who may have fallen victim to this scam should consider notifying the IRS. The IRS has established a special email notification address specifically for employers to report Form W-2 data thefts. Information about the procedure for submitting such reports, as well as the full text of the latest IRS notice to employers regarding this scam, is available here.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email