Safeguarding Your Company from Cyber Tax Crimes - Take Action Now!

By Jonathan D. Klein / Feb 06, 2017

As if tax season was not bad enough, the U.S. Internal Revenue Services ("IRS") recently issued an urgent alert warning that cybercriminal phishing scams are utilizing a new, more dangerously effective method for large-scale thefts of sensitive tax information from tax preparers, businesses, and payroll companies. Once cybercriminals have this sensitive tax information, they may be able to commit a multitude of crimes affecting millions of people, including filing fraudulent tax returns, identity theft, or both.

Previously, cybercriminals used various spoofing techniques - when a malicious party impersonates another user - to disguise an email to appear as if it was from an organization executive. Commonly referred to as business email compromise or business email spoofing, this email was usually sent to an employee in the payroll or human resources departments requesting a list of employees and their Form W-2s. The goal of course was to obtain sensitive tax information of employees of a company.

Now, a new variation of this scam is appearing earlier in the tax season and affecting a broader cross-section of organizations, including school districts, tribal casinos, chain restaurants, temporary staffing agencies, healthcare, and shipping and freight. In the latest twist, cybercriminals are following their prior request with an email from an "executive" to payroll or the comptroller seeking a wire transfer to a certain account. Thus, if successful, cybercriminals are not only gaining sensitive tax information, but also money.

As IRS Commissioner John Koskinen stated, "[a]lthough 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." It is for this reason, this scam is being described as "one of the most dangerous email phishing scams [the IRS has] seen in a long time." Indeed, where the FBI previously estimated that prior spoofing techniques netted cybercriminals approximately $3.1 billion, that number is now likely to dramatically increase under this revised method.

Because of the great potential for large-scale distribution of employee Form W-2 information and wire transfers, employers should **warn their employees now** and consider creating an internal policy about the use and transmission of Form W-2 information and wire transfers.

The FBI also suggests a two-step authentication system for emails to verify significant banking transactions. By implementing this extra security measure, businesses may reduce the risk of tax-related theft and the subsequent loss of sensitive tax information and money.

According to the IRS, organizations receiving a W-2 scam email should forward it to phishing@irs.gov and place "W-2 scam" in the subject line. Organizations that receive such scams or fall victim to them should file a complaint with the Internet Crime Complaint Center at www.ic3.gov, operated by the FBI. Likewise, 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.

Early preparation and planning and training are critical to thwart increasingly sophisticated cybercriminals. The risks are simply too great to avoid taking action now. If you are unsure how to protect your company or want to discuss how to implement a Form W-2 information and wire transfer internal policy, an experienced and knowledgeable attorney can help. Please contact Jonathan Klein at (215) 640-8535 | jklein@clarkhill.com or another member of Clark Hill's Cybersecurity team if you have any questions.

 |