THE
NATIONAL LAW REVIEW

'Tis The Season…For Dangerous W-2 Phishing Scams

Thursday, February 16, 2017

For each of the last few years, February and March have seen a sharp increase in the frequency and volume of W-2-related phishing scams. According to a recent IRS Notice, 2017 is no different, except perhaps that the threat is evolving.

Traditionally, the W-2 scam works like this:

> Cyber criminals use social engineering to identify certain key Human Resources (HR) and/or accounting personnel within a company. Targeting those HR and/or accounting employees, the cyber criminals send emails with a "spoofed" sender address. The emails appear to come from the company's CEO or other executive, and they generally claim that the CEO has an urgent need for Form W-2s for all employees in advance of a meeting the CEO has with the IRS. Unsuspecting mid-level HR and accounting personnel send on the W-2s, and inadvertently cause a data breach.

Article By Polsinelli PC
Daniel L. Farris Polsinelli On Privacy

Communications, Media & Internet
Tax
Labor & Employment
All Federal

The W-2 phishing scam is particularly dangerous for a number of reasons. First, the information contained in W-2s can be used for a wide range of crimes stemming from identity theft. Second, because the IRS and state taxing authorities have traditionally had difficulty identifying identity-related fraud, the cyber criminals can use electronic systems to file fraudulent tax returns in order to secure improper tax refunds. "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, this particular W-2 phishing scam, which debuted last year, is now evolving in a number of ways. The phishing scam "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." In another twist, "the cyber criminal 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 is advising organizations that receive a W-2 scam email should forward it to phishing@irs.gov and place "W-2 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.