Abstract: A growing number of businesses have been victimized by W-2 phishing scams by which criminals trick business owners or employees into divulging sensitive personal data. This article explores how the crime works and what employers can do to stop it.

Heed the warning signs of W-2 phishing scams

A growing number of businesses have been victimized by W-2 phishing scams. In a traditional phishing scam, a criminal tricks someone into providing confidential information and then uses it to steal money and/or the victim's identity. The W-2 phishing scam is a variation on this.

Whether you're a business owner, work in management or are simply an employee, it's important to be able to recognize this dangerous ploy. The better educated a company's employees are, the less likely that it will suffer at the hands of these criminals.

How it works

In a W-2 phishing scam, cybercriminals send emails to company employees — typically in payroll, benefits or HR departments — that claim to be from management. The emails request a list of employees along with their W-2 forms, Social Security numbers or other confidential data.

Here are some examples straight from the IRS:

- "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)?"

If the employee responds with data, criminals can use the information to file fraudulent tax returns in the employees' names, seeking refunds.

The scam is particularly nefarious because the employees it targets probably believe that, in complying with the emailed instructions, they're doing exactly what they're supposed to. Moreover, at first glance, the emails typically appear legitimate. Many contain the company's logo and the name of an actual executive, typically gleaned from publicly available information.

The increasing number of such scams prompted the IRS to issue an alert in 2016: "IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s." More recently, in November 2017, the agency issued another stern warning on its website, entitled "Employers, Payroll Officals: Avoid the W-2 Email Scam."

Education is key

While these scams have become more prevalent, businesses (and other employers) can take steps to reduce their risks. Because the scams target humans, rather than the technology itself, education is key. Inform all employees, and particularly those in areas

that handle sensitive data, of the scams. Remind them not to click on links or download attachments from emails that were unsolicited or sent by those they don't know.

Employees often are nervous about questioning a request that appears to come from upper management, so encourage them to double-check any request for sensitive information, no matter who appears to be making it. They should do this not by responding to the email in question, but by talking with a trusted supervisor or colleague.

Precautions necessary

With sensible precautions, your company can reduce the risk of falling victim to a W-2 phishing scam. Contact us for the latest information about any tax-related fraud issues.