ALERT: NEW SMALL BUSINESS SCAM STEALS KEY INFORMATION

This past month at least 55 companies reported they had fallen victim to a new type of specialized phishing scheme. It involves a criminal masquerading as a real employee, often a key executive, and then duping unwitting employees to provide payment or secure files. The scam takes many forms. Here are a couple of the most common.

THE SCAM

The W-2 request. Criminals send emails that appear to be from high-level executives to employees in their human resources department. The email requests PDFs of employees' W-2 forms or other personal information. Often the requests come when the HR department is busy complying with IRS reporting deadlines, so employees don't question whether they're legitimate requests. Once criminals obtain the employees' information, they use it to file fraudulent tax returns. To make matters worse, unlike other scams where a link to a bogus website may look somewhat correct but is actually a letter or two off, these scams will display the email address of the company executive perfectly.

Pay the fake vendor. In a similar ploy, businesses are victimized by "urgent" emails, supposedly from an executive, asking to have money wired to a fake vendor. Sometimes the sender claims to be an IRS agent who requests personal information or demands immediate payment of a nonexistent tax bill.

WHAT TO DO

Whenever confidential information is requested, employees should take a moment to ask members of the HR or payroll department if they know about a request for W-2s. Employees who receive a request should call the executive to confirm the request. Remind employees that the IRS never initiates contact regarding a tax issue by email or phone call. This scam can take many forms, so your best defense is making your team aware.

(1704)