Keep yourself safe from payroll and employee scams

From: www.forbes.com

The Internal Revenue Service (IRS) recently issued a warning about an uptick in phishing emails involving payroll direct deposit, wire transfer, and W-2 scams. The emails, which are primarily targeted to businesses, are not limited to a particular industry or employer - though the IRS has received reports that tax preparers are among those affected.

How they typically work:

The emails generally impersonate a real company employee, often an executive, and are sent to payroll or human resources (HR) personnel. The email asks the payroll or HR department to change the employee's deposit for payroll purposes and provides a new bank account and routing number which, of course, leads to a bogus account operated by the scammer. By the time the deception has been discovered, the employee has lost one or two payroll deposits.

In another version, the emails impersonate a company executive and are directed to the company employee responsible for wire transfers. The email requests that a wire transfer be made to a bank account for company purposes, but is actually controlled by the scammer.

In yet another version, the emails impersonate a company executive and requests information about forms W-2 from payroll or HR. The emails typically ask for the forms W-2 and earnings summary of all W-2 employees, or an updated list of employees with their personal details including Social Security Number, home address, and salary. The purpose of this scam is to allow thieves to quickly file fraudulent tax returns for refunds.

These scams are sometimes referred to as business email compromise (BEC) or business email spoofing (BES) scams. All businesses should be alert to these BEC/BES scams; they can take other forms, too, including fake invoice payments, title escrow payments, wire transfers or other schemes that result in a quick payoff for the thief. Businesses should consider policy changes to guard against such losses.

If you receive a suspicious email, read it carefully before taking action. A common theme in these and other email scams is that they include grammar and spelling mistakes.

Stolen/altered check scams:

While not an email scam, another thing to look out for at your workplace is stolen and altered check payments. Companies are reporting an increase in stolen vendor payments. These checks are typically stolen right out of a company's incoming or outgoing mail, and then the routing and account numbers are used to create new checks. It's important to be diligent about mail handling to prevent checks from being stolen.

What to do if you are scammed

If you receive a scam email, forward it to your company's IT department - they will know the proper way to handle scam emails, and can take steps to prevent reoccurance. No matter what kind of bogus email you receive, NEVER click on any links or respond to or engage with the scammers. Use common sense, remain alert and when in doubt, assume it's a scam.