

4-Asbury Park Press-IRS

Email from boss might be identity fraud scam

David P. Willis

Did the big boss send you an email asking for employees' Social Security numbers and salaries?

Careful. It's probably a scam.

The IRS has alerted people who work in payroll and human resources of an email scam that purports to be from company executives who are requesting employees' personal information. Criminals can use stolen data to commit identity theft or file fake tax returns for refunds. These types of emails, called phishing, use spoofed email addresses to make them seem legitimate.

So far, a few New Jersey companies have fallen for it. In a recent interview, Dave Weinstein, New Jersey's director of cybersecurity, said in one week, two companies have reported that scammers were able to get their hands on "personally identifiable information of employees and customers." He could not provide further details. He said the state may probably "see more as we get closer" to the April 18 tax deadline.

MORE: 5 uncommon steps to protect your identity

"These are cyber instances that don't involve any malware whatsoever and can be completely avoided by promoting better awareness at the user level," Weinstein said. "What it highlights is that there is a deficit of awareness in most organizations outside of the IT department when it comes to cyber security."

According to blog, Krebs on Security, payday lending company Moneytree has alerted former and current employees of that their tax data – including Social Security numbers, salary and address information, was accidentally given to scammers.

“Moneytree was apparently targeted by a scam in which the scammer impersonated me and asked for an emailed copy of certain information about the company’s payroll including team member names, home addresses, Social Security numbers, birthdates and W2 information,” Moneytree co-founder Dennis Bassford wrote to employees, according to the blog.

MORE: 4 new scams you’ve never seen before

These emails can be tricky. According to the IRS here’s what they may say:

“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).”

“I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.”

The IRS has seen a 400 percent in phishing and malware attacks so far this tax season.

Employees should be vigilant and double check requests for personal information, even if it’s from the boss. Scammers can use the Internet to find executives’ names.

MORE: No free Disney trip; beware social media scams

“If it doesn’t sound right, step back and verify,” said Special Agent Robert Glantz, a spokesman for the IRS Criminal Investigations’ Newark field office. “Verify that the person who sent you the email is really the person who sent it. Pick up the phone and call the CEO, call the CFO, whoever is emailing you and say, ‘Is this you?’”

There’s a good chance the answer will be no.

David P. Willis: 732-643-4039; dwillis@gannettnj.com;
facebook.com/dpwillis732

[View Comments](#)

[View Comments](#)

[Careers](#) [Staff Directory](#) [Accessibility](#) [Support](#) [Site Map](#) [Legals](#) [Our Ethical Principles](#) [Terms of Service](#) [Privacy Policy](#) [Your California Privacy Rights / Privacy Policy](#)

[Do Not Sell My Info / Cookie Policy](#)