No April Fool's Joke: New Scam Targeting HR And Payroll

Insights
4.01.16

An unfortunate number of employers have recently fallen victim to a phishing scam that tricks them into disclosing highly sensitive employee information to unknown third parties. Make sure to warn your Human Resources and Payroll Departments to be on the alert so that your company doesn't get added to the ranks of the swindled.

The Latest Scam

In the wake of tax season, multiple businesses have reported receiving spoofing emails, usually sent to Payroll and Human Resources personnel. The emails appear to be requests from high-level company executives, including in some instances the CEO, requesting that employee W-2 tax forms be transmitted to them for various administrative purposes. In reality these emails are phishing expeditions sent by data thieves, who use cloned company email addresses with authentic-looking company logos, colors, and signatures.

If the unsuspecting recipients are deceived into thinking the emails are legitimate, they will comply with the request and end up delivering W-2 forms to the scam artists. These forms contain a treasure trove of employee personal data, including Social Security numbers and other personally identifiable information. The successful hackers often use the data obtained from this phishing scam to file fraudulent tax returns on behalf of company employees.

You May Have Been Hacked And Don't Even Know It

The IRS has reported a 400% increase in phishing and computer malware incidents this tax-filing season, and many companies that have been compromised still don't realize it. In the coming weeks, as your employees attempt to file tax returns, you may learn that they are unable to file because someone else has already submitted a tax return on their behalf. The source of this data breach may be your company.

What You Should Do

You should immediately warn your employees about the risks associated with this new scam. You should specifically train your Payroll, Human Resources, and any other group of employees with access to personal identifiable information to be on the lookout for these phishing attempts or other red flags, such as requests for information not typically requested, or requests from individuals with whom the employees do not typically directly communicate. You should also take active security steps to ensure that personal data is only transmitted using secure methods.

If you believe your company is a victim of this scam, you may have a legal obligation to follow applicable data breach notification requirements. Besides determining your legal responsibilities, which vary from state to state, you should consider encouraging your employees to monitor their credit reports and take all of the usual measures to prevent identity theft. You should also suggest they file their tax returns as soon as possible in an effort to avoid the filing of fraudulent tax returns on their behalf.

If you have any questions about this situation, or how it may affect your business, please contact your Fisher Phillips attorney or any member of our Privacy and Cyber Practice Group.

This Legal Alert provides an overview of a developing situation. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Heather Zalar Steele
Partner
610.230.2134
Email

Service Focus

Privacy and Cyber