ARIZONA
EMPLOYMENT LAW LETTER
Part of your Arizona Employment Law Service

May 2016

Scammers, posing as execs, go phishing for data

by Dinita L. James
Gonzalez Law, LLC

Data security concerns are keeping more and more corporate executives up at night. The IRS isn't helping employers rest any easier, and the insomnia is spreading from the C-suite to the HR department.

On March 1, 2016, the IRS issued an alert, specifically addressed to HR and payroll professionals, warning them to beware of an emerging phishing e-mail scheme requesting personal information on employees that purports to be from company executives. As of that date, such schemes already had fooled several payroll and HR offices to e-mail cybercriminals payroll data, including W-2 forms that contained Social Security numbers and other personally identifiable information.

"This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments,", IRS Commissioner John Koskinen said in a written statement. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees.",

Sprouts didn't get IRS memo

Days after the IRS alert, Sprouts Farmers Market fell victim to this phishing variation known as a "spoofing", e-mail. Diego Romero, spokesman for the Phoenix-based grocery chain that operates 220 stores around the United States and employs more than 21,000 people, confirmed to news organizations that the company payroll department was tricked the week of March 14 into sending 2015 W-2 information to an unknown person.

"The criminals sent a phony email to [our] payroll team that looked like it came from one of our senior executives,", Romero told employees. Anyone who received a W-2 from the company for 2015 is potentially affected by the data breach, including the more than 3,000 employees of Sprouts' 30 Arizona stores and corporate offices.

Criminals exploit stolen personal information by filing fraudulent tax returns for refunds, for example. Sprouts is offering employees personal identity-theft services and a sincere apology and is cooperating with the IRS and the FBI investigations of the cybercrime.

Pick up the phone

Data security covers a wide range of technical issues but also requires a healthy dose of common sense. Spoofing e-mails will contain the actual name of the company's CEO and will be sent to a specific employee in the payroll office. Here's the actual, ungrammatical text of some spoofing e-mails, as reported by the IRS:

- "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 e-mail them to me asap.",

Common sense and the healthy dose of skepticism our digital society demands should prompt any low-level payroll staffer who received such an e-mail directly from a corporate executive at least to ask his boss what he should do. But we don't rely on "should", in today's business world. We train on it and on the need for everyone to be alert for cybersecurity risks.

Even if an e-mail of this kind is addressed to the chief HR officer who normally deals directly with the requesting executive, so much raw personal data about employees should never be sent to anyone without confirming that it will be secure. At a minimum, call and speak directly with the executive or her assistant to confirm the request.

Executives must encourage caution to protect sensitive employee data and welcome confirmatory inquiries. IT should respond quickly to inquiries, regardless of whether a specific e-mail checks out as genuine. All of us, and especially HR, have new roles and responsibilities in fighting cybercrime in the 21st century.

Dinita L. James is a partner with Gonzalez Law, LLC, in Tempe and the editor of Arizona Employment Law Letter. You can reach her at dinita.james@gnzlaw.com or 480-565-6400.