THIS WEEK'S SPECIAL REPORT

LAW/ACCOUNTING & TAXES

How Safe is Your Employees' Personal Information?

Employers must take immediate action

ELIZABETH A. HARTNETT
Viewpoint

The IRS issued an alert on March 1 to payroll and HR professionals about a new phishing scheme involving W-2 information. Employers need to take immediate steps to confirm the security of their employees' personal information.

The alert describes a scheme that has already claimed several victims. Payroll and human-resources officers have mistakenly emailed payroll data including W-2 forms that contain Social Security numbers and other personally identifiable information to cyber criminals who posed as company executives.

"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. "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."

The fraudulent email contains the name of the company CEO and requests a list of employees and information including Social Security numbers from a company payroll employee or outside HR service.

The IRS alert identified the following details included in these emails:

- Kindly send me the individual 2015 W-2 (pdf) and earnings summary of all W-2 forms 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, and salary).
- I want you to send me the list of W-2 copies of employees' wage and tax statements 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.

Criminals use this information to file fraudulent tax returns for refunds or otherwise monetize the stolen data.

We recommend that every employer take immediate action to address this phishing variation known as "spoofing." Employers should contact their outside human-resources professional to determine that security protocols are in place to avoid this cybercrime. In-house, you should conduct a review of data-protection policies, procedures, and technologies. Carnegie Mellon University's list of best practices for mitigating cybercrime is a helpful resource. See http://www.cert.org/insider-threat/best-practices/index.cfm.

This review should be team-based including management, HR, IT, and legal counsel. Heightened awareness of everyone in the organization may be the first and best protection. ■

Elizabeth A. Hartnett, Esq., CPA, is a partner at the Syracuse law firm, Mackenzie Hughes LLP. Her areas of expertise include family business entities, business tax and succession planning, pre-nuptial and post-nuptial agreements, fiduciary compliance, investment counsel, estate planning, fiduciary services and estate settlement. This viewpoint is drawn from the law firm's Plain Talk blog.