Published on *The National Law Review* https://natlawreview.com

Train Your Team: Protect Personally Identifiable Information From a Widespread Phishing Scam

Article By:

Danielle Vanderzanden

Every January 31, employers scramble to meet the deadline for mailing W-2 forms to their employees. This year, a new iteration of an old W-2 phishing scam surfaced immediately thereafter. In the 2017 version, scammers posing as a company's CEO or other high-level executive target human resources (HR) and payroll professionals with email messages requesting certain W-2s or all of a company's W-2s.

The email messages appear authentic and the associated email address actually looks like the email address of an executive authorized to receive such information. Hitting reply and attaching W-2s, however, sends the requested W-2s directly to the scammer, who then can use the W-2s themselves and all of the information they contain in a myriad of nefarious ways.

This scam became so popular in 2016 that the Internal Revenue Service (IRS) alerted payroll and HR professionals to be aware of the threat. At that point, the IRS noted that, "Criminals using personal information stolen elsewhere seek to monetize data, including by filing fraudulent tax returns for refunds." Unfortunately, the IRS's notice and last year's incidents of the scam have not prevented its recurrence, and similar spoofing email messages are rampant again this tax season.

To protect your company from the liabilities associated with these scams, the business disruption caused by testing the efficacy of your data breach response plan (your company has one, right?), and the hit to employee productivity that such events cause, employers should consider promptly taking some of the following steps:

- Share this article with all employees who have access to personally identifiable information (PII) so they know about the scam and can avoid becoming the next victim.
- Ensure that all employees who have the ability to send PII by email refrain from replying to email messages seeking PII. Instead, require that they always draft new email messages in which they personally type the email addresses of the recipients or pull the recipients' email addresses from their own contacts.
- Limit transmission of PII to encrypted email messages, and communicate the encryption code by a method other than email.

- Require that transmission of PII occur only after two employees have evaluated the request and confirmed the request's authenticity and appropriateness.
- Train employees so that they are familiar with the steps they can take to determine not only the published name of the sender but also the sender's actual email address.
- Ensure that your company constrains authorization to access PII with effective technical, physical, and logistical barriers.

Be prepared to take the following steps if you encounter this scam or any data breach:

- Ensure that you respond as legally required within the applicable time frames.
- Thoroughly investigate and document the incident.
- Promptly remedy the circumstances that led to your breach. Implement protective, multi-disciplinary, physical, logistical, and policy/process controls to prevent further disclosures and mitigate future risk.
- Provide law enforcement with required notices.
- Provide legally required notices to any individuals whose PII was disclosed.
- Provide identity-theft protection to affected individuals.
- Respond to inquiries from law enforcement, affected individuals, and media in an appropriate manner.

National Law Review, Volume VII, Number 47