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

# Phishing Alert: Employee W-2 Information at Risk

Article By:

Dena M. Castricone

Daniel J. Kagan

It's happening again. This time last year, there were a substantial number of phishing attacks all over the country targeting employee W-2 information. According to the IRS, phishing and other schemes jeopardizing tax information were up over 400% in 2016. The phishing attacks typically involve HR or payroll department employees sharing highly sensitive W-2 information with criminals who purport to be the CEO, CFO or other high ranking official using a spoofed email. The spoofed email commonly requests the sensitive W-2 information for all employees. At a quick glance, the email may look authentic. In many instances, the request for the information appears to be urgent, which forces the employee to act quickly and, many times, to provide the requested information by replying to the email. The criminals then take the information, file fraudulent tax returns or otherwise use the sensitive data for financial gain.

These attacks are incredibly disruptive to employees, extremely expensive for employers and are completely avoidable. All employees (and vendors) with access to W-2 information should be notified that these attacks are prevalent, especially at this time of year. Employees should be trained to carefully examine emails for signs of phishing. Some tell-tale signs can include the actual email address from which the message originates, *e.g.*, the email listed after the spoofed address, or the use of odd or overly formal language. The company also should implement a policy that any email request for W-2 information must be verified regardless of the apparent urgency in the message. Further, any such sensitive information that is emailed in response to a verified request should be sent through a new message created by the sender to ensure that the appropriate recipient receives the message (*i.e.*, do not reply to the emailed request).

In the unfortunate event that your company falls prey to one of these attacks, swift action is required. The disclosure of the information will trigger notice, reporting and other obligations under data breach laws, which vary by state. In most cases, the state laws that apply depend on the residency of the individual impacted. Therefore, many breaches involve the need to comply with the laws of multiple states.



National Law Review, Volume VII, Number 30

Source URL:https://natlawreview.com/article/phishing-alert-employee-w-2-information-risk