MURTHA CULLINA

NEWS ALERT

INFORMATION SECURITY & PRIVACY

Phishing Alert: Employee W-2 Information at Risk

By Dena M. Castricone & Daniel J. Kagan | January 30, 2017

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.

If you have any questions about a phishing attack or a data breach, please contact:
Dena M. Castricone at 203.772.7767 or dcastricone@murthalaw.com
Daniel J. Kagan at 203.772.7726 or dkagan@murthalaw.com

With more than 100 attorneys in six offices throughout Connecticut, Massachusetts and New York, Murtha Cullina LLP offers a full range of legal services to meet the local, regional and national needs of our clients. Our practice encompasses litigation, regulatory and transactional representation of businesses, governmental units, non-profit organizations and individuals.

Burt Cohen, Chair
203.772.7714
bcohen@murthalaw.com

Heather O. Berchem
203.772.7728
hberchem@murthalaw.com

Meredith C. Burns
860.240.6105
mcburns@murthalaw.com

Dena M. Castricone
203.772.7767
dcastricone@murthalaw.com

Michael P. Connolly
617.457.4078
mconnolly@murthalaw.com

Daniel J. Kagan
203.772.7726
dkagan@murthalaw.com

Rachel Snow Kindseth
203.772.7774
rkindseth@murthalaw.com

Bruce L. McDermott
203.772.7787
bmcdermott@murthalaw.com

James F. Radke
617.457.4130
jradke@murthalaw.com

Stephanie Sprague Sobkowiak
860.772.7782
ssobkowiak@murthalaw.com

Ryan M. Suerth
860.240.6157
rsuerth@murthalaw.com

David R. Sullivan
617.457.4156
drsullivan@murthalaw.com

Suzanne Brown Walsh
860.240.6041
swalsh@murthalaw.com

Edward B. Whittemore
860.240.6075
ewhittemore@murthalaw.com