MURTHA CULLINA

NEWS ALERT

PRIVACY & CYBERSECURITY

'Tis the Season: W-2 Phishing Scams Likely to Resurface After the New Year

By Dena M. Castricone and Daniel J. Kagan | December 13, 2017

W-2 phishing season is just a few weeks away. For the past several tax seasons, cyber criminals have duped hundreds of payroll departments into providing W-2 information on their employees, which results in the filing of fraudulent tax returns and other identity theft issues. These attacks are incredibly disruptive to employees, extremely expensive for employers and are completely avoidable with some training.

The typical W-2 phishing email purports to be from a high-level executive and asks the payroll employee to provide W-2 or other tax-related information either by replying to the phishing email or by sending the information to another email address. In many instances, the request for the information appears to be urgent, which forces the employee to act quickly. These messages can be very convincing. The emails often contain the actual signature block of the executive or a different indicator that makes the employee believe that the email is authentic.

Employees should be trained to examine emails carefully for signs of phishing and to think twice before sending any sensitive information. Some tell-tale signs can include an unfamiliar email address (e.g. president@ceo.gmail.com instead of the president's actual email address: dsmith@abc.com) or the use of odd or overly formal language. Companies should also implement a policy that either no W-2 information will be requested via email or require that employees verify any email request for W-2 information regardless of the apparent urgency in the message. Verification could include contacting the sender via telephone or by starting a new email thread to confirm the validity of the request. Finally, 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).

The IRS has instructed organizations receiving W-2 scam emails to forward them to phishing@irs.gov and indicate "W2 Scam" in the subject line and also to file a complaint with the FBI's Internet Crime Complaint Center (IC3) at https://www.ic3.gov/default.aspx.

In the unfortunate event that your company falls prey to a W-2 or other phishing attack, you should contact legal counsel immediately to assist in implementing strategies to minimize damage and to determine legal obligations. Immediate action is the key to minimizing damage in W-2 phishing attacks as well as all other data breach situations.

If you have any questions regarding phishing attacks or any other data or cybersecurity issue, please contact:
Dena M. Castricone at 203-772-7767 or dcastricone@murthalaw.com or
Daniel J. Kagan at 203-772-7726 or dkagan@murthalaw.com.

Dena M. Castricone, Chair
203.772.7767
dcastricone@murthalaw.com

Burt Cohen, Vice Chair
203.772.7714
bcohen@murthalaw.com

Michael P. Connolly
617.457.4078
mconnolly@murthalaw.com

Michael J. Donnelly
860.240.6058
mdonnelly@murthalaw.com

Melissa A. Federico
860.240.6042
mfederico@murthalaw.com

Daniel J. Kagan
203.772.7726
dkagan@murthalaw.com

Rachel Snow Kindseth
203.772.7774
rkindseth@murthalaw.com

Paul E. Knag
203.653.5407
pknag@murthalaw.com

Bruce L. McDermott
203.772.7787
bmcdermott@murthalaw.com

James F. Radke
617.457.4130
jradke@murthalaw.com

Stephanie Sprague Sobkowiak
203.772.7782
ssobkowiak@murthalaw.com

Ryan M. Suerth
860.240.6157
rsuerth@murthalaw.com

Suzanne Brown Walsh
860.240.6041
swalsh@murthalaw.com

Edward B. Whittemore
860.240.6075
ewhittemore@murthalaw.com

Kristen L. Zaehringer
203.653.5406
kzaehringer@murthalaw.com