It's Tax Season – Is Your Scam Alert on? (Update)

Mar 30, 2017

Categories:

Publications

Authors:

Michael E. Nitardy

John S. Wagster

In January, we alerted clients that 2017 would likely yield a new crop of phishing emails sent by fraudsters looking to steal employees' W-2 information. Three months into the year, we can unfortunately report that our prediction was correct. Emails impersonating CEOs and asking for hard copy lists of W-2s have been hitting their mark and leaving HR managers wringing their hands.

Phishing is any attempt to acquire sensitive information or steal money from you or your company. Most phishing is email-based and it is extremely effective 95% of all infections in an organization start with a phishing email.

An especially damaging form of phishing email called CEO Fraud or Business Email Compromise (BEC) targets HR and finance departments. In a BEC phishing campaign, attackers impersonate high level executives, usually the CEO, and send urgent sounding emails to individuals primarily in the HR and finance departments, since they handle payments and/or have access to employee data. Such attacks result in employees being tricked into transferring large sums of money or sending sensitive employee data to an attacker-controlled account.

Wire transfer fraud has been a problem for years, but in 2016 a new form of BEC fraud began that focused on stealing employee W-2 data, not money. Below is an example of a W-2 fraud email. This simple email has been extremely effective in stealing W-2 information from companies across all industries:

> *Hi [Internal Finance Person],*
>
> *I need you to send me the list of W-2 copy of all employees' wage and tax statement for 2016. Kindly prepare in PDF file type and email me the file.*
>
> *[CEO]*

BEC fraud owes its success to "spoofed" email addresses – attackers have ways to make emails look like they are coming from

a person inside an organization. It can be difficult to tell without looking at the technical components of the email address whether the originating address is valid. One should be suspicious of any email that is requesting one to send sensitive employee data or wire transfer funds.

Outside of BEC fraud, there are indicators that can help determine if an email is a phishing email. Some of these include:

- Poor grammar in the body of the email.
- Incorrect spelling.
- The "from" address is clearly not the sender's email address.
- If the email contains a link, the destination of the link (the URL) does not match the link name.

Takeaways:

- Alert employees about the phishing email indicators.
- Make clear they will NEVER receive an email from anyone within your organization, including senior management, requesting that they send employee W-2 information or wire transfer large sums of money.
- Provide guidance on whom to notify immediately if an employee receives such an email and instruct them to then delete it.
- Instruct employees to NEVER click on a link or a document attachment within any suspicious email without the approval of your information security manager.

For more information, contact Michael Nitardy, John Wagster, or any other member of Frost Brown Todd's Privacy & Data Security Team.

FBT Gibbons