Privacy and Data Security
ALERT
Fox Rothschild LLP
ATTORNEYS AT LAW
March 2016

Latest Cyberattack Targets Workers With Access to Sensitive Data

By Mark G. McCreary, Partner and Chief Privacy Officer

Businesses have come under increased assault through cyberattacks known as "spear phishing" scams, and more and more of those businesses have turned from target to victim. A new twist in this scam takes advantage of the busy tax season, the desire to promptly respond to purported upper management, and social engineering employees in order to target only employees with immediate access to sensitive employee data.

Spear phishing attacks are virtual traps set up by criminals who, in this case, send emails to employees that appear to come from actual, upper management. Typically they are well written and look authentic. Usually, there is some explanation or pressing reason offered for why personal information is required. Lately, the targets have been payroll and human resources personnel.

Tax season has likely been partly responsible for the "surge in phishing emails seen this year," according to an IRS alert issued on March 1 that warned payroll and human resources professionals about emails purporting to be from company executives requesting employees' personal information.

"Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees."

The IRS bulleted some of the requests contained in these fake emails:

- Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review.
- Can you send me the updated list of employees with full details (name, social security number, date of birth, home address, salary).
- I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me ASAP.

No organization is immune from spear phishing. A large social media provider recently issued apologies and will offer two years of identity theft insurance and monitoring after one of its workers inadvertently released sensitive company payroll information to a criminal. The unidentified employee opened an email that appeared to be from the victim company's CEO. Although none of

the company's internal systems were breached and no user information was compromised, hundreds of employees have had their personal information exposed to the public.

Almost 11,000 employees of a health system had their personal information compromised in a spear phishing scam where a criminal similarly posed as an organizational executive in an email. The unsuspecting employee gave the criminal personal information related to all employees, though, thankfully, no information related to patients. The victim said that it discovered the breach only after the IRS released its general alert.

The FBI has also warned the public and has published suggestions for avoiding becoming a spear phishing victim, including the following tips:

- Keep in mind that most companies, banks, agencies, etc., don't request personal information via e-mail. If in doubt, give them a call (but don't use the phone number contained in the e-mail — that's usually phony as well).
- Use a phishing filter. Many of the latest web browsers have them built in or offer them as plugins.
- Never follow a link to a secure site from an email. Always enter the URL manually.
- Don't be fooled (especially today) by the latest scams.

More of these attacks should be expected as tax season winds down, so organizations should be vigilant about ensuring that all employees are aware about phishing scams.

For more information about data security, contact Mark McCreary, the firm's Chief Privacy Officer and a member of the Privacy and Data Security practice group, at mmccreary@foxrothschild.com or 215.299.2010.

Fox Rothschild LLP
ATTORNEYS AT LAW