FARM CREDIT

FRAUD PROTECTION AWARENESS SERIES

Fraud Tip #1 – CEO Email Scams

One of the most successful fraud techniques targeting businesses today is known as the "CEO Email Scam." The scammer effectively impersonates a company's CEO or other high-level executive by gaining access to or "spoofing" his or her email account, and requesting a wire transfer. According to the FBI, between October 2013 and August 2015, over 7,000 U.S. businesses fell prey to this scam, netting criminals an estimated $747 million. The scam has been reported in all 50 states and in 79 countries.

The CEO Email Scam

With some basic computer hacking skills, this can be a simple and effective scam:

- A fraudster takes over or "spoofs" the business or personal email account of a high-level company executive, such as the CEO or CFO. Spoofing involves the creation of a fake email account that closely resembles a legitimate one. For example, the valid email address CEO@company.com could be spoofed as CEO@c0mpany.com, where a zero (0) is used in place of the O in "company."
- The fraudster sends an email to a company employee who is likely to be responsible for outgoing payments, requesting that a wire transfer be sent to a certain payee, and including the necessary account and bank information. In another variation, the fraudster, impersonating the CFO, "forwards" a second fake email from the CEO requesting the wire transfer - lending even more credibility to the request.
- The employee – believing that he or she is fulfilling a legitimate request from a high-ranking executive – instructs the company's financial institution to initiate the transaction.

Why CEO Email Scams Are Effective

- *If a scammer has gained access to an executive's email account, they can read other emails and determine the tone, language or jargon the executive typically uses.* It was once relatively easy to spot a scammer's email by the use of poor grammar and misspelled words. Not any more – criminals have learned they need proper grammar in order to be believable.

- *Scammers do their research.* They send other emails or place calls to a company to find out exactly who is responsible for outgoing payments. They may also research the organization in general and refer to other known employees, customers or suppliers – or use company jargon – to give the targeted employee more confidence that the request is real. A scammer might even submit the request when the executive is out of town, anticipating that the executive will be difficult to reach and less likely to provide a personal confirmation of the request.
- *CEO email scams succeed because they are based on techniques of "social engineering" – manipulating a person into doing something or giving away information by creating a belief that they are communicating with a known and trusted person.* Instead of hacking into a computer system based on its technological vulnerabilities, they target human vulnerabilities – sincere people who are eager to fulfill an important request and do a good job. Social engineering is all about establishing credibility and trust.
- *Scammers are adept at creating a strong sense of purpose and urgency.* The email wire request may express that the payment has to be made on an "emergency" basis or to "avoid losing a valued customer." Or, maybe the employee is being brought into an executive's inner-circle by requesting a payment related to a "confidential deal."

How to Detect and Prevent CEO Email Scams

Look for "red flags":

- Is it unusual to receive an email payment request directly from this executive?
- Is the request coming from an executive's personal rather than business email account?
- Are outgoing payment requests normally submitted with certain paperwork that is not present?
- Is the payment being requested for an existing vendor or customer, but with new bank account information?
- Is the payment to a new vendor or customer? Is the new vendor a type of business your company would normally pay for goods/services?
- Is the transaction for an unusually high amount – especially for the vendor or customer?

- Is the payment being sent internationally, especially to a country in the Asia-Pacific region (China, Malaysia, Hong Kong) or Eastern Europe? Authorities say these are common destinations for such transactions.
- Is the timing of the payment request out of the ordinary?

In any of these cases, you should consider calling the executive to verbally confirm the request or ask a superior to verify the request for you. Either way, pay attention to your concerns and speak up about them! Set up a standard procedure requiring phone confirmation of any payment request received by email.

Also consider minimizing the information you publish on your website or other social media about employee activities that could allow criminals to pinpoint when executives are traveling or otherwise out of the office.

Although there is no certainty that a particular course of action will prevent a loss, the considerations outlined above might be beneficial to you. Please keep in mind that your company might be responsible for a loss even if it is related to a fraud perpetrated on the company. In the scenario described above, for example, because an authorized employee of the company provided the wire instruction to the bank, the company is responsible for the wire even if the employee was deceived by the fraudster.

As you consider the fraud awareness information described above, please also bear in mind your important role in the fraud detection and reporting process. Your vigilance in reviewing your accounts and transactions is vital to fraud prevention and detection. Fraud schemes – as well as loss recovery efforts and outcomes – can be complicated. Early detection and prompt reporting of a fraud is critical because the passage of time might adversely affect the potential recovery of a fraud loss or the outcome of a customer claim. Your attentiveness often is the first line of defense to a fraud, and if a fraud occurs, your diligence might aid in a potential loss recovery.