FARM CREDIT

FRAUD PROTECTION AWARENESS SERIES

Fraud Tip #10 – Social Engineering

We continue our quarterly series of fraud prevention tips with a discussion of *social engineering*, which is the fraudster's art of manipulating people into providing confidential information.

Social engineering manifests in many different ways and through many oddly-named fraud techniques, including phishing, vishing, smishing and others. The foundation of social engineering – and the reason fraudsters succeed – is through the ability to manipulate a target into believing that an email or a telephone request is legitimate. This is usually accomplished by directing the victim to respond with a sense of urgency to the new contact information cited in the email or phone call.

Fraudsters use social engineering because exploiting our general *human tendency to trust* and *desire to help others* is often much easier than hacking a company's computer system. The good news is that there are a number of ways to protect yourself and your company from becoming victimized.

Common Methods of Social Engineering

Phishing
Phishing refers to an attempt by fraudsters to obtain sensitive information (user IDs, passwords and banking information) by email. Phishers send emails purporting to be from colleagues, customers, vendors, banks or other recognized parties. Based on the recipient's familiarity with the email sender – and the trust implied by the relationship – the recipient may willingly provide the information the fraudster is seeking.

Spear Phishing
As the name implies, spear phishing is a highly targeted form of phishing. Fraudsters target a specific person within an organization who, based on their research, performs a specific duty and may have bank account information and access.

Vishing/Caller ID Spoofing
Vishing (think: voice phishing) is phishing conducted by telephone. Vishing attempts may come in the form of a direct call from a fraudster – purporting to be from a bank – asking for confirmation of account information under the guise of a credit issue or even a fraud alert. *Yes, fraudsters will use a fraud warning to commit a fraud scam!*

Vishing may also take the form of an automated call requesting a call back to a specific number and then asking for confidential information.

Many vishing attacks use caller ID spoofing. With this technique, a fraudster can manipulate a caller ID system by changing the actual originating telephone number to any other number. A call appearing to be from a familiar or local number adds legitimacy to the scam.

Smishing
Smishing (think: SMS phishing) is the text message version of phishing. These text messages often provide a web link or telephone number that the recipient must use to take care of a supposedly urgent issue. The executable web link installs malicious software on the user's device, or the call-back number may request confidential account information that must be provided immediately to "address" the issue.

Impersonation Scams
Impersonation scams continue to be one of the most successful fraud techniques used against companies today. 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 creating a fake email account that closely resembles a legitimate one. For example, the valid email address JDOE@COMPANY.COM could be spoofed as JDOE@COMPANY.COM, where a zero (0) is used in place of the O in "company."

In addition to spoofing, impersonators can also "mask" their actual email address so that the message appears to be from the impersonated individual. Reviewing the internet headers in the email properties of the original email may show a different, "masked," Reply To email address.

Fraudsters may also send an email to an employee who is likely to be responsible for outgoing payments *(see spear phishing above)* requesting that a wire transfer be sent to a certain payee, and including all the necessary account and bank information. Their hope is that the employee will believe that the request is real – and will respond to the sender's "urgency" – and complete the wire transfer.

Fraudsters also commonly conduct impersonation scams using established customer and vendor names.

Why Social Engineering Scams Are Effective

- *Social engineering succeeds by establishing a false basis for familiarity and trust.* Fraudulent emails have information, names or logos/graphics that are familiar to the recipient.
- *Social engineering targets human vulnerabilities and eagerness to be responsive and do a good job.* Instead of spending time hacking into a computer system based on its technological vulnerabilities, fraudsters capitalize on human nature and our innate desire to help solve problems.
- *Urgency is another reason for the success of social engineering.* Requests for "confirmation" of account information are often made under the guise of solving a problem – such as *"someone is using your credit card without your knowledge"* – which are threatened to worsen if not addressed immediately.
- *Fraudsters do their research.* Particularly with spear fishing and impersonation scams, fraudsters examine the targeted company's website to find names of employees and customers to make their communication appear legitimate. They may phrase their emails using website language or industry jargon to create a façade of knowledge and familiarity. They also may scan business networking sites, such as LinkedIn, for particular employee titles, in order to target certain individuals. And, they may supplement their research by reviewing personal social media sites – Facebook, Instagram, Twitter, etc. – to find more information that will help them establish trust with their targets.

How to Detect and Prevent Social Engineering Scams

- *Have a healthy suspicion of, and independently confirm, any request for confidential information or sending of funds.* Always verify any request by calling the company or person, using a telephone number that you know to be real – not one provided in an email or call. As well, never reply to the same email address from where the request originated – you may be simply asking the fraudster to confirm its legitimacy!
- *Slow down.* By establishing a heightened sense of urgency, fraudsters want you to act, not think. While some situations do indeed require urgency, it is also a significant red flag for potential fraud. Even when time is of the essence, take the time to confirm sensitive requests with known people and entities, through an independent method (telephone or different email account).

- *Trust your instincts! Pay attention to red flags and unusual circumstances and ask yourself these questions:*
  - Does this email "sound like" other emails you have received from your CEO or other company executive?
  - Does this email from your bank sound and look like other emails you have received from them previously? Is the bank's logo missing, out of place or look fuzzy (have rough edges)? Is this email formatted differently? Are there obvious grammar or spelling errors? Even if the email looks right, take the time to independently confirm any request for confidential information.
  - Does an internal email request for an outgoing funds transfer fall outside of your company's standard practices for such requests? Even if standard procedures are being followed, confirm the payment with the requestor by telephone – not by replying to the original email.
- *Carefully check the email domain portion of an email sender's address* – the portion between @ and .com (or .net, etc.) – for any replacement characters, such as 0 (zero) instead of the letter O or l (lowercase letter L) in place of I (uppercase letter I). Keep in mind that many other character replacement variations are commonly used. Even requests from domains that appear to be legitimate should be independently confirmed with the requestor.
- *Be selective of the information you post on your business and personal social media sites.*

As you consider the fraud awareness information provided 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 incident 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 for fraud, and, if a fraud incident does occur, your diligence might aid in a potential loss recovery.