Social Engineering Fraud

By Michael Brown, CIC, CRM

There is a good chance that any given one of you reading this article knows what social engineering fraud is. Email fraud is an example of one of the most common schemes used in social engineering. Since the COVID-19 pandemic began, the number of cyber-attacks has dramatically increased. According to the FBI, there are between 3,000 and 4,000 complaints of cyber-attacks a day. For example, your controller receives an email from the president of the company directing them to wire money and they complied. The email reads:

"Hi Bob - I need you to do something right away. As you know, I'm visiting the Smoky Mountains this week with the family so short on time. We have an opportunity to make a small acquisition that would be a great fit. I've known this guy since I was at Rapid Transit. I'm under an NDA so please don't discuss with anyone at this point. Please wire $50,000 in earnest money to the below account. I'll fill you in on the details when I return next week. Regards, Mary"

The level of detail involved made the email sound very convincing. Everything made sense due to the fact Mary was in the Smoky Mountains for the week with her family, she worked at Rapid Transit 15 years ago and she was returning the following week. The NDA was not out of the norm. On top of that, the email address and style looked legitimate down to the signature block and disclaimer. Mary *always* signs her email messages "Regards, Mary". The request to wire money was a bit out of character but not totally beyond reason. Bob didn't really want to bother Mary with questions when she was taking her first vacation with the family in two years and after going through a quarantine. Therefore, he complied only later to find out Mary made no such request.

Another common scheme is very similar, but this time the email request comes from one of your most reputable vendors and advises that they have changed banks. The email simply asks that future payments be made using the new account details. Again, the misleading elements revolve around a personal story such as prior employment. "I've decided to change banks to the one I used to use when I was at Speedy Transfer."

In both cases, the minutiae created credibility, so nothing seemed terribly out of the ordinary. As I discuss this issue with clients, I generally receive one of three responses. About 20% of the time the response is "we've never had that happen but how could the controller do that." The rest of the responses are about evenly split between "somebody tried that on us, but our controller would never do that" and "yeah, that happened to us and we lost about $60,000." Although the amounts involved tend not to be huge, they do sting. Collectively however, if 30-40% of brokers and forwarders are losing money to this scheme, it ***IS*** a big deal.

You can and should have insurance to protect you when something like this happens. It is usually purchased along with a broader set of coverages that also protect your company from things like cyber breaches, ransomware, and crime events but often is not included unless specifically added.

Things you can do right now to protect yourself

A quick look at Facebook and LinkedIn can often provide a scammer with just about everything they need to know to perpetrate the fraud including your work history, vacation destinations, etc. If they obtain an email sent by you, the scammer will often get a glimpse of your writing style as well as your signature block and any disclaimers. etc. Cloning or "spoofing" the sender's email address is child's play to most cyber scammers. In summary, think about how much you share online on social media and with what level of detail.

Implement protocols between senior management and those in your organization with the authority and ability to send money that would require a verbal verification of written requests from management or vendors. With vendors, prior to sending any funds to a different bank, be sure to contact them using previously established phone number(s) and not the number provided in the questionable email.

Unfortunately, the frequency of these scams is continuing to increase but with some good risk management techniques and proper insurance coverage, the chance of a loss can be significantly reduced.

Don't wait until you are a victim to find out if you have coverage. For more information on our Cyber Defense Package, contact your local Avalon representative or click here: https://www.avalonrisk.com/cyberliability.html.