February 22, 2017

Social Engineering Fraud

Social engineering techniques are being used by fraudsters to manipulate vendor payments. In recent months these techniques have been used to target public-sector entities, such as municipal governments and public universities. In these instances the fraudsters will send a request to update routing and account information for ACH or wire transfer. The request may ask that the payment method be updated from payment by check to ACH or wire transfer.

These social engineering scenarios are similar to the Business Email Compromise scams. The difference between the Business Email Compromise scam and the social engineering scenario is that Business Email Compromise scam targets the company CEO or CFO and orders a payment be made. The social engineering scenario involves a fraudster impersonating a legitimate contractor and orders a change in payment information. Like the Business Email Compromise scam, the social engineering scenarios can result in funds being transferred anywhere in the world.

While any organization can be the target of a fraud attack, public-sector entities can be more vulnerable since their contracting information is generally a matter of public record.

Any request for changes to payment instructions should be verified. The Commerce Bank “Best Practices for Corporate Banking” brochure, which is available within the Commerce Connections® Help Menu, provides guidance for mitigating your risk of becoming a victim of fraud. In addition consider the following when initiating any ACH or wire transfer payment:

- Establish clear, written policies and procedures for authenticating intra-company ACH or wire transfer requests communicated via email, fax, or phone.
- Through the compliance with business policies, use out-of-band authentication procedures to verify ACH or wire transfer change requests from vendors. Procedures may include a call-back to the vendor to obtain verbal verification or establishing a phone Personal Identification Number (PIN) to verify the vendors identity.
- Be cautious of any ACH or wire transfer request which expresses a high degree of urgency or the need for confidentiality which may be aimed at making the payment request difficult to authenticate.
- All new ACH or wire requests or changes to payment beneficiary information should be verbally confirmed with the requestor using a phone number previously on file with your organization. Never use the phone number included with the ACH or wire transfer request.
- Limit the number of employees within your organization that have the ability to initiate or approve an outgoing payment.
- Look carefully for small changes in email addresses that mimic legitimate email addresses. For example, .co vs. .com, abc-company.com vs. abc_company.com, or hijkl.com vs. hjkl.com. If you receive an email that looks suspicious, forward it to your IT department for review.
• Spread the word. Coach your employees about this type of fraud and the warning signs. Be suspicious and diligent, and encourage employees to ask questions.

Always carefully and thoroughly verify transactions for authenticity and promptly reconcile accounts. If you believe any transactions are in error or were unauthorized, please contact Commerce Bank immediately at 800-207-0886.