Federal Authorities Issue Warnings on New Form of Fraud Known as “Executive Impersonation”

One of the newest forms of fraud threatening corporations of all sizes is known as “Executive Impersonation.” This type of scheme involves an individual hacking into an organization’s email and posing as a senior level executive, often the CEO or CFO. They issue a fraudulent email, which appears to come from the executive, and instruct an authorized employee to urgently execute a financial transaction, such as a wire or ACH transfer.

Often, they claim the funds are for confidential situations, such as an acquisition, and tell the employee to speak with no one in the office regarding the transaction for legal reasons.

Who does “Executive Impersonation” happen to?

Consider the scenario faced by ABC Company, a small, family-owned business with approximately 100 employees.

One afternoon, the Comptroller received an email addressed from the CEO but sent by a fraudster who had hacked into the organization’s email system. The email instructed the employee to wire $400,000 to an attorney the CEO was dealing with to acquire an overseas company. The e-mail emphasized the confidentiality of the acquisition.

After several e-mail exchanges with the “CEO”, the Comptroller, who had individual authorization to complete financial transactions on behalf of the company, initiated the international wire to the account number provided in the e-mail.

Per normal procedures, the company’s bank completed a call back to the Comptroller to confirm the wire was initiated by the client and not an outside party. The Comptroller verified that they did initiate the wire, however, the bank had no way of knowing the wire request was actually originated by an impersonating fraudster and not the CEO/CFO.

As a result, the transaction was processed and the company only became aware of the fraudulent activity when the CEO noticed a large, unauthorized draw on one of the corporation’s accounts. This type of impersonation fraud happens to companies every day and results in large financial losses for the victim.
Steps to Limit “Executive Impersonation”

I. DUAL AUTHORIZATION/VERIFICATION

Many organizations unknowingly take on the type of fraud risk related to “Executive Impersonation” by seating financial decision making with a single individual, such as the Comptroller in the previous case study. Regardless of size, employee tenure, etc..., companies should always require dual authorization and separation of duties to mitigate outside risk from penetrating the organization.

In addition, any emails requesting the creation or change of wire payment instructions should be verified by phone. Employees should use a dependable verification channel, such as a telephone number from an employee directory, to validate new wire payment instructions because hacked emails could contain fraudulent contact information.

II. EDUCATION

“According to security experts, although implementing security controls and enhanced authentication can help stop these attacks, educating employees against these socially-engineered schemes is one of the best ways to defend against this new form of fraud.” (“Masquerading: Federal Authorities Issue Warnings Regarding New Form of Wire Fraud.” securityworldexpo.com. 29 July 2014. Web.)

Fraudsters prey on organizations with a lack of fraud knowledge. Keeping all of your employees educated on the most current fraud trends is key to possibly preventing fraud before it occurs or recognizing it quickly to reduce an organization’s potential for loss.

III. CHOOSE THE RIGHT FINANCIAL PARTNER

Partnering with a financial institution that keeps you informed on fraud developments and is invested in helping to protect your organization from fraud is also key.

As a partner in fraud prevention, your financial advisor should:

- Keep you inform on relevant fraud industry data
- Provide help on identifying fraudulent activities early to reduce organization losses
- Advise you on fraud prevention best practices, such as using a stand-alone PC for banking or having internet service administrators perform user reviews on a quarterly basis to help improve internal controls and security. These reviews should include looking at your organization’s user roster, removing anyone that no longer requires access and updating active user’s contact information, especially e-mail addresses.
- Offer necessary fraud protection products and procedures, such as the dual authorization and the separation of duties, to reduce your risk of becoming a fraud victim.
- Help you to reconcile account activity daily
- Encourage out of channel verification of any payment

Overall, the right financial provider can help reduce the potential that certain types of fraud, such as “Executive Impersonation”, can have to penetrate your organization.

For more information, please contact your Treasury Management Consultant or Relationship Manager.