3 WAYS TO HELP PREVENT EXECUTIVE AND VENDOR IMPERSONATION

Fraud occurs every day to all types of organizations and still, it is easy to have the mentality that "It will never happen to my company." In today's volatile environment, educating yourself and your employees on the different types of fraudulent activity that exist in the marketplace is a crucial step in protecting your organization.

M&T Bank

FEDERAL AUTHORITIES ISSUE WARNINGS ON NEW FORMS OF FRAUD, "EXECUTIVE AND VENDOR 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 email accounts of senior level employees and posing as them, 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.

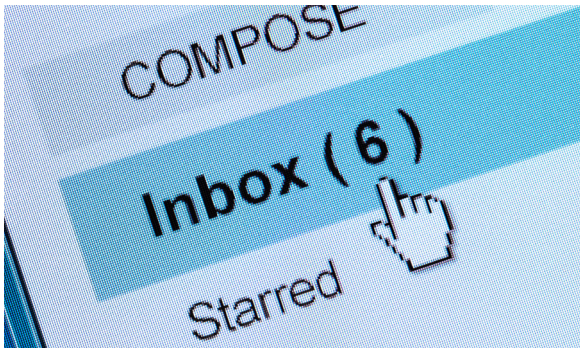
WHO DOES "EXECUTIVE IMPERSONATION" HAPPEN TO?

Consider the scenario faced by 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 his or her email account. The email instructed the employee to wire $400,000 to an attorney the CEO was dealing with to acquire an overseas company. The email emphasized the confidentiality of the acquisition.

After several email 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 email.

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.

The fraudster often claims the funds are for a confidential situation and tells the employee to speak with no one regarding the transaction.

RISE IN "VENDOR IMPERSONATION" FRAUD

Another common form of fraud is called "Vendor Impersonation." This scheme involves making a payment to what appears to be a legitimate and frequent supplier but the payment is sent to another, unintended recipient. This type of fraud is executed in a variety of ways but all result in a payment request that appears to come from a vendor that your organization is familiar with.

HOW DO FRAUDSTERS PULL OFF "VENDOR IMPERSONATION"

A criminal impersonates a business vendor and requests that your organization modify where future payments are sent (altering them from the traditional payments). Usually done by phone, email, or letter, the fraudsters are able to divert payments to their own accounts. A hacker can also breach the email account of an employee of the targeted company and study the pattern of payment requests received by its Accounts Payable department. The scammer then submits a fraudulent invoice that looks genuine except for minor changes to the payment instructions. Similarly, a fraudster can break into the accounts receivable system of an organization's vendor and generate a fraudulent invoice or payment request.

Consider what happened to a manufacturing company. The Accounts Payable manager at this company received an email that appeared to be from a long standing vendor. The email informed the company that they changed banks and payment should be made to a new account. The fake supplier uses an email signature that looks legitimate. The employee proceeds to change the bank details and a payment is issued.

Three months later the vendor advises the company's Accounts Payable department that they have missed the last three payments. The manufacturing firm advises that all payments have been made but the vendor confirms they never received them. An investigation reveals that the earlier email request was fraudulent and funds cannot be retrieved.

STEPS TO LIMIT "EXECUTIVE AND VENDOR IMPERSONATION"

I. DUAL AUTHORIZATION/VERIFICATION

Many organizations unknowingly take on the type of fraud risk related to "Executive and Vendor Impersonation" by seating financial decision making with a single individual, such as the Comptroller in the first 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 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 informed on relevant fraud industry data
- Provide help on identifying fraudulent activities early to reduce organization losses
- Advise you on industry 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 email 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

Fraud protection products and procedures can help reduce your risk of becoming a fraud victim.

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

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