RISK SIMPLIFIED

RESOURCES

PRISM Partner Program, Cyber Security – Synoptek

Multi-State Information Sharing and Analysis Center

California Cybersecurity Integration Center

California HTTAP Program

QUESTIONS

Email PRISM Risk Control
or call 916.850.7300

Cyber Smart: Vendor Impersonation Fraud and How to Avoid It

by Travis Clemmer, SMS

It's no secret that email based fraud attempts are on the rise. Commonly referred to as "phishing," this type of scam involves the sending of email impersonating a reputable company in an attempt to entice individuals into providing personal or confidential information.

One specific form of phishing impacting public agencies is vendor impersonation fraud. These fraud attempts typically seek to hijack payments to existing vendors through falsified payment routing methods. Victims of vendor impersonation fraud unknowingly pay the scammers in lieu of their vendors. Often times, these scams go undetected until the organization receives a legitimate lack of payment notice from its vendor or supplier.

Common Signs of Vendor Impersonation Fraud

- Scammers may provide an unexpected change of payment address or payment routing information for an existing vendor. More and more these requests have the appearance of legitimate business correspondence.
- Unexpected and excessively low prices for products may be a sign that a scammer is trying to bait

an employee into making a purchase.

- Scammers may try to create urgency in an attempt to encourage a fast transaction. Be on the lookout for limited time offers, or threats of impending price increases.
- Scammers may claim to be affiliated with, or a subcontractor to an existing business partner.
- As always, users should be aware of the other classic signs of phishing schemes including:
  - Poor spelling and grammar
  - Unfamiliar or unorthodox email addresses or web links
  - Lack of sender contact information

Tips to Avoid Falling Victim to Vendor Impersonation Fraud

- Carefully review all email correspondence, paying close attention to email addresses and email domains. Ensure the email domain matches that of the vendor.
- Only use known vendors, or vendors for which the organization has a pre-existing relationship.
- Call vendors to confirm any changes to payment routing information. Legitimate businesses will not discourage telephone communication.
- Never complete transactions via email with unfamiliar vendors.
- Report all suspected fraud attempts according to established organizational policies and procedures.
- Ensure all employees are trained to recognize fraud attempts and what to do if they suspect fraud is occurring.
- Route all purchases through a central person or department.

For any additional questions regarding this topic or related regulatory requirements, contact the PRISM Risk Control Department.