ACFE General Forum Posting

Posted 04-29-2021 12:54

Reply

Here's an interesting method I recently encountered that is intended to misdirect payments. Our client received an email purportedly from an oil & gas operating company that they did business with, requesting that all future payments be made electronically. The email was identical to many emails received over time from the operator, including the employee names, address, disclaimer info, etc., and even CC information for the company CFO. It looked totally legit, except that the email domain had been subtly modified. The actual domain "XXXchex.com" had been modified to "XXXclhex.com". The change was not identified as the email addresses were in small font size, and the lower case "L" blended into the vertical line of the "H".

After this email was received, all future correspondence went to the fictitious domain, since the recipient clicked on "reply" to the sender. Multiple emails went back and forth, including one with wire transfer instructions for the "new" payment method. Luckily, client's bank detected an anomolie in the router and account number, and rejected the wire request.

AP Internal Control TIP:

In addition to standard internal authorization procedures for updating payment addresses or accounts, any change in payment instruction to an existing vendor received via email or telephonically should be verified by a return telephone call with the company requesting it. The call should go to the vendor's main number rather than a direct number, and should be verified with the company controller, CFO, or other person OTHER THAN the person who sent the request. We've all fallen into the habit of just hitting "reply".

George Keeney CFE, CPA/CFF, CGMA
IFSG, Inc.