

Fraud Protection Awareness Series

Case Study: Spoofed Vendor Email Directs Payments to Fraudulent Account.

Please note that this case study represents an aggregation of actual scenarios brought to CoBank's attention, though company names have been changed.

Situation

Paragon Company experienced a business email compromise fraud attack. Employees at the company received emails purportedly from their vendor, Alert Corporation, requesting a change to their bank account information. Employees at Paragon Company complied with the email requests without calling the vendor to verbally confirm the new payment instructions and originated a large-dollar wire transfer to the vendor at the unconfirmed account.

Discovery and Resolution

The fraud was discovered when a legitimate representative for Alert Corporation made a courtesy call to the company to ask when they would be receiving their payment. Paragon Company informed this representative that they had made the payment already and that it went to Alert Corporation's updated bank account. Alert Corporation informed Paragon Company that they had not actually updated their bank account information.








Paragon Company promptly reported the fraud to its bank and a recovery claim was initiated immediately with the transaction recipient bank. Fortunately, only a short period of time elapsed from when the wire was sent and when the fraud was reported, so the funds were fully recovered. But that's not always the case – the more elapsed time between the payment and discovery of the fraud reduces the chances for full or even partial recovery. In many cases, even if the discovery is made moments after the wire is sent, recovery isn't guaranteed and the claim can take a long time to resolve with the counterparty bank.

Paragon Company has since implemented new internal controls requiring that employees call a previously known number for their vendor to validate new and/or modified payment instructions.

How it Happened

Paragon Company provided the bank with the fraudulent emails, and the subsequent analysis revealed that the emails originated from a spoofed email account. The fraudster created a domain that contained “r n”, which appears to look like an “m” in small print (e.g. @amex.com vs @arnex.com). The bank determined that the fraudster had created the spoofed email domain the day before the fraudulent emails were received by Paragon Company. The bank also reviewed the origination IP addresses from the fraudulent email requests and determined they originated in Abu Dhabi.

Watch for These Red Flags

-  Was there anything unusual about the email requesting the account change? [Is the tone out of character? Does the format of the email look different from previous ones? Does the email signature match previous ones?]
-  Is there anything unusual about the email address from which it came? Does it match previous emails exactly?
-  Carefully examine the domain portion of the email address to determine if the legitimate email domain has been spoofed. Lack of apparent evidence of a spoofed email should not be taken to mean the email is legitimate because impersonated emails can also be masked or hacked.
-  Does the email contain a fantastic story explaining why the account has to be changed? [For example, the account has been suspended due to a fraudulent check that was deposited.]
-  Be aware that there are many other ways for fraudsters to mask and spoof valid email addresses. [Always validate payment instructions via an alternate channel with a known vendor representative.]