Business Email Compromise Scam: Stories From Victimized Businesses

Nearly every financial institution we talk to has a story about a business client that has been victimized by the Business Email Compromise (BEC) scam. Here are just a few to highlight the variations and similarities across the attacks, and the effort criminals will put into these attacks to have the fraudulent requests look legitimate.

Scenario 1: Auditor Asks for Payment for Acquired Business

Victim: Controller at Employee-owned Commodities Trader

The corporate controller received emails that appeared to be from the company's outside auditing firm with requests to transfer millions of dollars to a Chinese bank. Three wire transfers were requested and sent for a total of $17.2 million. The initial email instructed a wire transfer of $780,000, the following day a request was emailed for $7 million and three days later a final request was received for $9.4 million. The initial emails include language focusing on secrecy, urgency and sensitivity, including:

> "I need you to take care of this. For the last months we have been working, in coordination and under the supervision of the SEC, on acquiring a Chinese company. ... This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations."

The Controller called the auditor to confirm, using the phone number provided in the email. The criminal was ready with a person in place posing as an employee of the auditing firm to confirm the requests. There also was an element of consistency between the wire requests and the company's business plans as the company had been discussing the expansion into China and they were in the middle of an audit. These factors put the wire requests and the request for sensitivity and secrecy in line with company business plans.

Additional details: http://www.omaha.com/money/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html

Scenario 2: Wire Transfer With Immediate Money Mule Action

Victim: Controller at Midsize Business

The Controller received email that appeared to be from CEO requesting a wire transaction to an individual in Pennsylvania. The $38,000 wire was processed on a Friday morning to bank A. Shortly after, the beneficiary went into bank A to request a wire transfer to bank B for $31,400, a second wire for $6,000 through Western Union, and then withdrew $600 in cash.

On Tuesday morning, the Controller received and submitted a second wire request, this time for $78,000. However the bank flagged the request only because of an invalid routing number. This request was to a business in Kansas. The bank contacted the requestor who, only when they went to look up the correct routing number realized that the request was a scam. If not for a typo on the part of the criminal, the business surely would have been victimized for an additional $78,000 instead of only being scammed for $38,000.

Scenario 3: Fraudsters Mined Email for How to Submit Wire Request

Victim: Bookkeeper at Midsize Business

This attack started with the criminal compromising the business' email system to look for details of how to submit a legitimate-looking wire request. It was also well timed.

The bookkeeper had just received approval via email from CEO to submit and approve wires. The next day the bookkeeper received a request from the CEO to submit a wire transfer request, which was consistent with how previous wire requests had been submitted. After receiving the transfer order, the bank called the company because the wire request seemed out of character, but the bookkeeper was insistent that it was a legitimate request and that it came from the CEO. The bank processed the payment before the business realized that it was a fraudulent request.

Scenario 4: Fraudster Pursues Victim to Get Paid Twice

Victim: Finance Department at Midsize Business

This attack started when the business received an email from a vendor explaining that they have changed payment instructions. New payments were to be sent to an account in China. The financial institution thought it looked suspicious and called to confirm, but the business insisted it was OK.

When the wire request came back "unable to apply" the business checked the wire instructions and submitted the wire request again, and this time the receiving bank did not reject it. Then the fraudster, posing as the vendor, called to say that they had not received payment yet, and the businesses submitted the wire request a third time, resulting in total payments exceeding $200,000.

Scenario 5: "Attorney" Calls with Wire Instructions

Victim: Two Victimized Businesses on the Same Day

The finance department of two different businesses received emails from their respective CEOs regarding company acquisitions that were top secret. The emails explained that an attorney working on the acquisition would send payment instructions. They subsequently did receive an email (from the fraudster), and it was from a real law firm adding legitimacy to the request. The "attorney" then called to provide wire instructions over the phone. The losses were averted when the FI called the CEOs to confirm.

Scenario 6: Spoofed Email Asked for Vendor Payment

Victim: Bank CFO

While a majority of the cases of the business email compromise scheme target businesses, this particular case was directed towards a bank. Talmer Bank's CFO received an urgent request from the bank's CEO for a $20,000 wire transfer to a vendor. The CFO viewed the request on his iPhone and wasn't able to see that the domain name in the email address included an extra "r" (…@talmerrbank.com instead of …@talmerbank.com). However, some awkward wording and a request for urgency alarmed the CFO. The well-trained wire staff reached out to the CEO to request validation at which point the bank learned that they had been a victim of the BEC scheme. Fortunately the money never left the bank.

Additional details: http://www.clickondetroit.com/news/bank-ceos-fake-email-and-the-russian-mob/35359592