Business Email Compromise Scam

The **FBI** has issued a warning about a significant spike in victims and dollar losses stemming from an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers. According to the FBI, *thieves stole nearly $750 million in such scams from more than 7,000 victim companies in the U.S.* between October 2013 and August 2015. In January 2015, the FBI had released stats showing that between Oct. 1, 2013 and Dec. 1, 2014, some 1,198 companies lost a total of $179 million in so-called **business e-mail compromise** (BEC) scams, also known as "CEO fraud." The latest figures show a marked 270 percent increase in identified victims and exposed losses. Taking into account international victims, the losses from BEC scams total more than $1.2 billion, the FBI said.

The victims of the Business E-mail Compromise range from small to large businesses. The perpetrators monitor and study their selected victims prior to initiating the BEC scam and are able to accurately identify the individuals and protocol necessary to perform wire transfers within a specific business environment. The fraudster is able to steal money with the help of an unwitting accomplice, an employee who is fooled into submitting a wire request. Two versions of this scheme are:

- Payment request from a company executive.
- Invoice from supplier or business partner via spoofed email address.

Best Practices for Businesses to Detect the Business Email Compromise Scam

October 2015

These best practices are based on the FBI alerts and conversations with financial institutions that have successfully detected this scam. This is a comprehensive list, and most businesses cannot practically implement all of these suggestions, but implementing those that are realistic and practical for your specific operations and resources will decrease the risk of being victimized by this scam.

Check

- Check to see if the request is consistent with how earlier wire payments have been requested. How often does the CEO or CFO directly request a wire payment?

Do they typically submit requests when traveling (these attacks often are timed when the exec is out of the office)? Have earlier requests included the phrases "code to admin expenses" or "urgent wire transfer," which have been reported by victims in some of the fraudulent email requests?

- Check to see if the payment is consistent with earlier wire payments – including the timing, frequency, recipient, and country to which prior wires have been sent.
- Be suspicious of requests for secrecy or urgency, and emails that request all correspondence stay within the same email thread, such as only use Reply, not Forward.
- Establish a company domain for company email instead of using open source email services such as Gmail. Businesses using open source email are most targeted. Register domains that are slightly different than the actual company domain and might be used by fraudsters to spoof company email.
- Look carefully for small changes in email addresses that mimic legitimate email addresses. For example, .co vs. .com, abc-company.com vs. abc_company.com, or hijkl.com vs. hljkl.com. If you receive an email that looks suspicious, forward it to IT for review.
- Program your email system to add "-e" to the end of all external senders' email addresses, thereby flagging email coming from domains that don't match the company domain. The system will detect minor changes to the domain name and flag it as external, making it easier for employees to detect fraudulent emails.
- If you don't need web access to email, turn webmail off as it provides another attack point for criminals. If you must provide web access to email, limit accessibility by implementing VPN or another security control.
- If the request is from a vendor, check for changes to business practices. Were earlier invoices mailed and the new one is emailed? Were earlier payments by check and they're now asking for a wire transfer? Did a current business contact ask to be contacted via their personal email address when all previous official correspondence used a company email address? Is the location or account to which the payment is to be sent different from earlier payments to that vendor?

Confirm

- Use an alternate mechanism to verify the identity of the person requesting the funds transfer. If the request is an email, then call and speak to the person using a known phone number to get a verbal confirmation. If the request is via phone call or fax, then use email to confirm using an email address known to be correct. Or Forward the email (instead of using Reply) and type in a known email address. Don't reply to the email or use the phone number in the email.
- While many people may be hesitant to question what appears to be a legitimate email from their boss or the CEO, consider which would be worse in light of how common this scam is: asking the CEO or CFO to reconfirm the request, or having the money stolen.

- Limit the number of employees who have the authority to submit or approve wire transfers.
- Implement dual approvals for financial transactions. If you do not have written procedures, develop them. Avoid having the two parties responsible for dual approvals in a supervisor/subordinate relationship as it could undermine the effectiveness of the process. Once they're in place, be sure to always follow established procedures.
- Use a purchase order model for wire transfers to ensure that all payments have an order reference number that can be verified before approval.
- For employees that frequently travel and are authorized to request funds transfers, develop a special way to confirm requests. Perhaps develop a coding method that isn't documented within the network (in case of an intrusion search).

Coach

- Spread the word. Coach your employees about this type of fraud and the warning signs. Alert receptionists, admins, and others not to provide executive's travel schedules over the phone to unknown callers. Be suspicious and diligent, and encourage employees to ask questions.
- Be careful what is posted to social media and company websites, especially reporting structure and out of office details. Criminals have been known to launch these attacks when they know the CEO or CFO is traveling and therefore not easily available to confirm the request.
- Slow down. Fraudsters gain an advantage by pressuring employees to take action quickly without confirmation of all the facts. Be suspicious of requests to take action quickly.
- Trust your financial institution. If they question a payment, it's worth a couple minutes to cooperate with them to confirm it's legitimate.
- Executives need to be tolerant, indeed supportive, of employees double-checking requests.

What to do if you're hit by the BEC Scam

Report the Attack

Businesses that have been victimized by the BEC scam (regardless of dollar amount), are encouraged to file a report with the IC3 at www.IC3.gov or contact their local FBI office.

Businesses also are encouraged to contact their financial institution to report the attack, ideally within 24-48 hours after which it is very rare that funds can be recovered.

Timing is critical. If notified immediately, financial institutions and law enforcement have a better chance of recovering the stolen funds, even if the funds were sent internationally. Waiting even 24 hours to report an incident can greatly diminish law enforcement's ability to recoup funds.

When reporting the incident, identify the complaint as "Business Email

Compromise" or "BEC" and provide:

- A general description of this crime, how and when it occurred
- Header information from the email message the executive sent internally to request the funds transfer
- The specific wiring instructions, including beneficiary and account details for where the transfer was to be sent
- Attempted and actual loss amounts
- Details on when and how you believe you were defrauded
- Other relevant information you believe is necessary to support your complaint

Keep all original documentation, emails, faxes, and logs of all telecommunications. You will not be able to add or upload attachments with your IC3 complaint if it's filed online; however, retain all relevant information in the event you are contacted by law enforcement.

Complete an Internal Review

Businesses are encouraged to conduct an internal review to determine how the attack occurred and if changes are needed. Specifically:

- Was the email system hacked, giving criminals access to executive's email accounts? If so, are additional protections in order?
- What actually happened, and who was involved? This may indicate where training is needed or if there might actually be an insider element to the attack, although this is rare.
- What allowed the attack to happen? Do processes and controls need to be revised to prevent such a loss again?

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.

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.