Best Practices for Businesses to Detect the Business Email Compromise Scam

October 2015

Guardian Analytics Fraud Intelligence

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?