Business Email Compromise: Best Practices for Prevention

What is business email compromise?

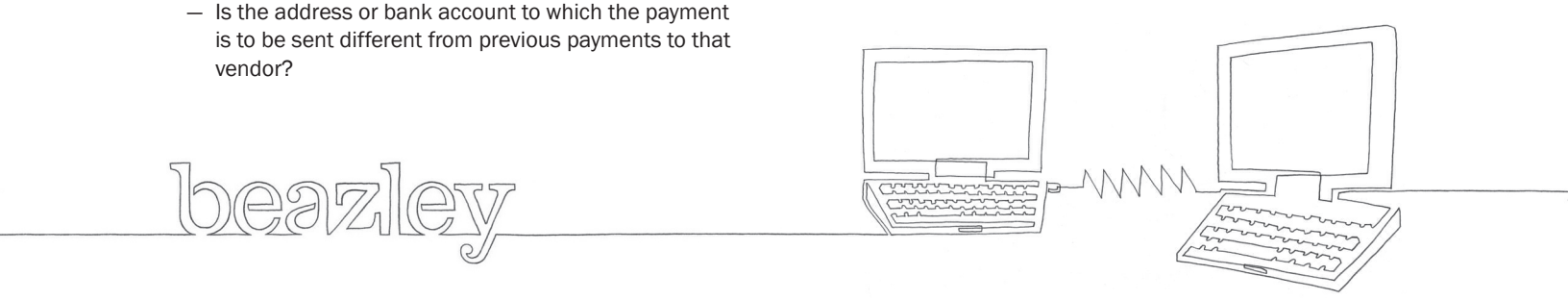
Business email compromise is a social engineering attack in which a cybercriminal uses compromised email credentials or spoofs a legitimate email address in order to induce an employee to make a wire transfer or other electronic payment to a bank account controlled by the cybercriminal or, in some cases, to transfer sensitive data such as W-2 forms.

What is fraudulent instruction?

Fraudulent instruction is the written or electronic instruction intended to mislead the recipient.

How can you reduce the risk of financial losses?

- For employees who frequently travel and are authorized to request funds transfers, establish a process to confirm requests. For example, set up a predetermined code that a request must include that is not documented within the network. (You don't want a criminal who has access to your network to be able to search for your process.)
- Provide periodic anti-fraud training that teaches employees to detect and avoid phishing and social engineering scams.
- If a vendor or supplier requests changes to its account details (including, but not limited to, bank routing numbers, account numbers, telephone numbers, or contact information):
  - Confirm all requests by a direct call to the vendor or supplier. Make sure to use a phone number the vendor or supplier provided *before* the request was received.
  - Before making any changes, send notice of receipt of the request to someone other than the person who sent the request.
  - Require review of all requests by a supervisor or next-level approver before making any changes.
- If the request is from a vendor, check for changes to business practices:
  - Were earlier invoices mailed while the new one was emailed?
  - Were earlier payments by check and now the request is 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 address or bank account to which the payment is to be sent different from previous payments to that vendor?
- Be suspicious of 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.
- If the request is for a funds transfer, confirm that the request is consistent with how previous funds transfer instructions have been requested:
  - Does the CEO or CFO directly request a wire payment?
  - Is the request consistent with earlier wire payments – including the timing, frequency, recipient, and country to which prior wires have been sent?
- Establish an ***out-of-band verification process*** to confirm the identity of the person requesting a funds transfer:
  - If the request is by email, then call and speak to the person using a pre-established phone number to get a verbal confirmation.
  - If the request is by phone call or fax, then use email to confirm using an email address known to be correct.
  - Instead of using "Reply," forward the email and type in a known email address.
  - Do not reply to the email or "verify" using the phone number in the email. If the request is fraudulent, the criminal will have supplied fake contact information, too.
- Limit the number of employees who have the authority to submit or approve wire transfers.
- Establish dual approvals for financial transactions. The two parties responsible for dual approvals should not have a supervisor/subordinate relationship as it will undermine the effectiveness of the process.
- Implement ***two-factor authentication*** for remote access to your email system.
- If you do not have ***written procedures***, develop them.



CBSL557_US_05/18