Be aware: recognizing a business email compromise scam

Business Email Compromise (BEC) is defined as a sophisticated scam targeting businesses that regularly perform wire transfer payments. These types of fraudulent activities are an increasing menace to small, medium and large businesses globally. To help you recognize the characteristics of these threats, two of the most common variants of BEC scams are outlined below. Each narrative is a fictitious account based on real-world events.

Scenario one: The CEO impersonation

The most common variant of the BEC scam. It requires the least amount of effort to be successful.

Pre event

In preparation to target “Computercorp” for their next scheme, the fraudsters:

- Perform reconnaissance, identifying the management structure as well as key individuals within the company who are the most likely to process financial transactions.
- Use Google and LinkedIn searches like “Computercorp controller” and “Computercorp CEO” to identify the key individuals, including the CEO “Judy Exec” and Controller “Henry Ledger”.
- Identify the email naming format for the company through additional searches, and discover Judy is on vacation through her social media account.
- Create a lookalike domain (cmputercorp.com) through an online marketing company that offers free trial domain registration and hosting. They then set up a lookalike email address (judy.exec@cmputercorp.com) to leverage during the impersonation.
- Generate a PDF with payment instructions to an account owned by them.

Scenario one: The CEO impersonation (continued)

The scam

The fraudsters initiate the communication to the Computercorp controller, Henry Ledger, beginning the fraud scheme.

Initial email from fraudsters	*From: Judy Exec <judy.exec@cmputercorp.com>* *To: Henry Ledger <henry.ledger@computercorp.com>* *Subject: Urgent payment* *Henry,* *What is the cutoff time for wires? I need to have this payment sent ASAP.* *<Attached: PaymentInstruction.pdf>* *-Judy* *Sent from My iPhone*
Response from controller	*From: Henry Ledger <henry.ledger@computercorp.com>* *To: Judy Exec <judy.exec@cmputercorp.com>* *Subject: Re: Urgent Payment* *Judy,* *Wires must be processed prior to 2:00 PM PT. How should I code the transfer?* *-Henry*
Final response from fraudsters	*From: Judy Exec <judy.exec@cmputercorp.com>* *To: Henry Ledger <henry.ledger@computercorp.com>* *Subject: Re: Urgent payment* *Please code to my admin for now. Thanks.* *-Judy* *Sent from My iPhone*

- With this information, Henry initiates the wire transfer to the fraudsters' account. Dual authorization is required. So, the secondary approver calls Henry, who confirms that the request came directly from the CEO and is urgent. The secondary approver also approves the wire.
- The money is sent to the fraudsters' account.

Post event

- Judy Exec, the CEO, returns from vacation and Henry sends her a note to reconfirm the allocation of the funds from the previous wire.
- Judy calls Henry immediately, claiming that she did not send any instructions for a wire.
- Henry contacts their bank to request a funds recall. The bank initiates the recall; however, the funds have already been moved from the fraudulent account and are no longer available.
- Computercorp contacts their local FBI field office and reports the fraudulent event to the Internet Crime Complaint Center (IC3).

In the aftermath of the event, Computercorp strengthens their wire authorization controls by implementing callback procedures for all requested wire transactions.

Scenario two: The payment instruction switch

Another scenario involves fraudulently changing a known supplier's payment instructions to divert funds to an account owned by criminals or their accomplices.

Pre event

An organized crime group targets "ABC Corp.", a U.S.-based global manufacturing company that makes frequent wire payments to foreign suppliers for goods and services. The group:

- Identifies one of ABC Corp.'s Asia-based suppliers, "XYZ Supply."
- Compromises the email accounts of several XYZ Supply account reps who are using weak passwords in their webbased email solution, which has no secondary authentication.
- Search through the email for payment requests to customers of XYZ Supply and notice an invoice to ABC Corp. for goods, with an additional request for goods to be invoiced in the near future.

The scam

- The criminals email the supplier manager at ABC Corp., via the most recent XYZ Supply email chain requesting a change in payment instruction.
- The email does not alert the supplier manager given it is legitimately from the XYZ Supply email account.
- The supplier manager updates the payment system with the new account information assuming the email was legitimately sent from XYZ's account representative.
- ABC Corp. receives the goods and pays via a wire to the fraudulent account provided by the criminals.

Post event

- The day after payment, the supplier manager at ABC Corp. emails the account representative at XYZ Supply to notify them of the payment. The account representative responds that the wire was not received.
- The controller checks the outgoing wires report to confirm the wire was sent, and ABC Corp. discovers the wire was sent to a fraudulent account.
- The controller at ABC Corp. calls their bank to request a funds recall, but the funds are no lo nger available in the receiving account and cannot be recalled.

ABC Corp. and XYZ Supply split the cost of the loss, and later implement additional controls around payment instruction changes including callback confirmation procedures. XYZ Supply also commits to implementing stronger security controls on their web-based email system, including multi-factor authentication.

Recap and defense

These scenarios depict situations that could have been avoided through stronger internal controls. In both cases, a phone call directly to the requestor via a verified number could have avoided the situation. While these situations vary in degrees of sophistication, stronger controls around email must also be part of every business' security strategy. Keep in mind that traditional email should not be considered a trusted communication mechanism when dealing with critical activities such as money movement.