5 Tips for Payments Staff:
Help Protect Your Business Against Business Email Compromise (BEC) Scams

As a payments employee, criminals will target you by pretending to be your CFO, CEO or a trusted contact at a known vendor. Try these five best practices to help protect your organization from BEC attacks.

1 Be wary of external emails

Handle emails from outside your organization with extreme caution, especially ones that ask you to click a link or open a document. If you do not recognize the sender or are not expecting the communication, do not click any links or open any attachments and immediately notify your IT or information security department.

2 Look closely at email addresses

Examine email addresses in the reply field to confirm they match the exact spelling of the originating company's domain and the individual's name. Fraudsters frequently use deceptive lookalike domains to trick victims. They may also use compromised email accounts, which can only be detected by performing a trusted callback to confirm the validity of the email.

$1.7B

in losses to BEC in 2019 alone[1]

3 Read emails carefully

Be highly suspicious of any email relating to payments or accounts that uses urgent language or provides excuses for the lack of a callback option. Other common examples of BEC red flags and pressure tactics include poor grammar, punctuation, spelling and words such as "kindly send" or "kindly respond."

CHASE J.P.Morgan

4 Perform a callback

Always perform a callback to the person making a request using a phone number from a system of record when setting up a new account, processing a request for payment, changing payment instructions or changing contact information.

Essential Elements of a Callback

- Confirm all of the account details, including the new account number.
- Do not confirm payment instructions only via email – always perform a call back using a phone number from a system of record to the person making the request.
- If a callback is not currently a part of your company's payment control process, try to implement one or escalate the issue to someone who can.

What to Do If You've Been Attacked

If you do fall prey to a BEC scam, immediately notify your bank of the fraud, fill out a report with IC3.gov and contact your local FBI field office. The longer you delay in reporting the attack and engaging with the FBI, the lower your chances of getting your funds returned.

5 Follow up on suspicious transactions

If you receive a call from your bank about a suspicious transaction, pay close attention to the information provided and reconfirm that your organization performed all applicable controls, including a callback. Clients often confirm payments as valid only to later report them as fraudulent.

For more resources on how to protect your organization, visit
jpmorgan.com/cb/cyberfraud-protection

1 FBI's Internet Complaint Center (IC3) 2019 Internet Crime Report