5 Tips for Payments Staff to Help Protect Against Business Email Compromise Scams

Payments staff are often the front-line defense against business email compromise (BEC)—a pervasive method of fraud that has only grown more rampant during recent years and caused $1.7 billion in losses in 2019 alone.1

As a payments employee, criminals will target and try to trick you by pretending to be your CFO, CEO or a trusted contact at a known vendor. Below are five tips to help you protect your organization from becoming the next victim of BEC.

1. 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 on the link or attachment and immediately notify your IT or information security department. Getting users to click on links or attachments is a common tactic fraudsters use to take control of email accounts, which enables them to read emails and impersonate employees and business partners.

2. Examine the characters in email addresses carefully 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.

3. Be suspicious of any email relating to payments or accounts that uses urgent language, excuses for the lack of a callback option, poor grammar, punctuation or spelling and words such as “kindly send” or “kindly respond.” These are common examples of red flags and pressure tactics of BEC scammers.

4. Always comply with your own internal control procedures for establishing or revising accounts payables records. In addition, always perform a callback using a phone number from a system of record when you receive a request for payment to a new account or a change in payment instructions. When performing a callback:
   - Confirm all of the account details, including the new account number.
   - Do not confirm payment instructions only via email—always perform a callback using a phone number from a system of record.
   - 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.

5. 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.

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.

For more information, please contact your Chase or J.P. Morgan representative or visit: chase.com/cb

© 2020 JPMorgan Chase & Co. All rights reserved. Chase, J.P. Morgan and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, “JPMC”) and if and as used herein may include as applicable employees or officers of any or all of such entities irrespective of the marketing name used. This does not constitute a commitment by any JPMC entity to provide any product or service. All trademarks, trade names and service marks appearing herein are the property of their respective registered owners. Products and services may be provided by commercial bank affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those which can be provided by commercial bank affiliates under applicable law will be provided by registered broker/dealer affiliates such as J.P. Morgan Securities LLC, J.P. Morgan Institutional Investments Inc. or by such other affiliates as may be appropriate to provide such services under applicable law. Such securities are not deposits or other obligations of any such commercial bank, are not guaranteed by any such commercial bank and are not insured by the Federal Deposit Insurance Corporation. Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMC and/or its affiliates/subsidiaries. 704437

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