Defending Against Business Email Compromise

Business email compromise (BEC) fraud is conducted by sophisticated organized crime groups who use email to trick your employees into sending fraudulent payments by impersonating your executives, business partners or vendors. BEC fraud can result in devastating financial losses for an organization.

We help clients combat fraud through ongoing education, using analytics to screen for anomalous payments, and working with clients to attempt to recover funds after fraud occurs. However, stopping fraud and potential losses takes more than just our team. You should also implement strong security protocols within your organization, such as:

- Regularly educate your executives and payments staff about BEC and how they can help prevent it.
- Implement robust payment and information technology controls.
- Develop a BEC response plan that includes prompt reporting of all instances of payment fraud to us. While there are no guarantees that funds can be recovered once they are sent, the faster a report of fraud is made, the better the recovery chances.

It is important to take phone calls from us regarding suspicious transactions very seriously. It could be your last chance to avoid becoming a victim. Commercial Banking clients are liable for all losses incurred for payment originating using any authorized users' security credentials or the credentials of others who have designated transaction authority.

We have prepared this guide to help you protect your organization. Inside these pages you will find:

- Strong callback validation procedures to help prevent fraud losses. Failing to do callbacks or doing them incorrectly can result in significant fraud losses.
- Recommendations on how senior leaders and management can help prepare their organization to combat BEC threats.
- Tools for payments employees to help prevent BEC.

Help Dial Back BEC

Help Dial Back Business Email Compromise

In the on-going fight against payments fraud, the only thing more important than performing a callback is doing it properly—here's how.

Sophisticated cybercriminals continue to steal large sums of money from organizations of all sizes through business email compromise (BEC)—but a proper callback process can help stop these schemes dead in their tracks. An appropriate process requires an employee, typically a payments staff member, to pick up the phone and validate new payment requests, requests to establish a new bank account, changes to payment instructions and changes to contact information.

Train your employees to:

- Follow controls for the validation of new or revised payment information.
- Understand how BEC scams work and what they can do to help prevent them.
- Never trust emails, texts, or unsolicited phone calls alone to authorize payment requests or change contact information.
- Escalate any concerns if a payment seems suspicious—even after performing a callback.
- Be very suspicious if a vendor offers vague reasons for changes to a new account, such as tax audits or current events, e.g., "Due to COVID-19, we need to update our payment information…"

IMPORTANT

Callbacks should be made to the actual person making the request using a phone number retrieved from a system of record.

- Be wary of vendors who frequently change payment instructions. Fraudsters will sometimes provide several different accounts to victims during a BEC fraud attempt.
- If you receive a call from your financial institution asking you to validate a suspicious payment, take it seriously. It could be your last chance to stop a fraudulent payment before it's too late.

CHASE

J.P.Morgan

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

Prepare Your Employees: Review, Train and Test to Help Prevent BEC Attacks

Prepare Your Employees:
Review, Train and Test to Help Prevent Business Email Compromise (BEC) Attacks

Try these six best practices to help safeguard your organization against BEC:

1 Review your email security practices

Talk to your senior technology leaders about:

- Multifactor authentication to provide additional security beyond usernames and passwords.
- Parameters to quickly detect email inbox forwarding rules that send all or selected emails to an external email address.
- Automatic labeling of external emails to help prevent the impersonation of employees.
- Robust email logging that can be leveraged for investigation in case of a successful BEC attack.

$1.7B

in losses to BEC in 2019 alone[1]

2 Train employees on BEC prevention

Teach employees how to identify and report suspicious emails relating to payment transactions. Stress the importance of performing callbacks to the person making the request, using a phone number from a system of record, for all payment requests, new accounts and account or contact information changes.

3 Test your employees regularly

Establish an employee testing program with phishing and BEC attempts that appear to come from your senior leaders and trusted business partners.

CHASE

J.P.Morgan

4 Standardize validation for payments and account changes

Establish with your customers and business partners how changes in account information will be communicated and validated. Also confirm how you expect them to validate changes to your banking information.

5 Create a social media policy

Construct, implement and enforce a social media policy that prohibits sharing details about company roles and responsibilities, so cybercriminals cannot develop a picture of your corporate structure, including addresses to target your employees.

6 Protect your web domain

Consider hiring a firm that will notify you of web domains that have been registered to deceptively look like your own; cybercriminals can use lookalike domains in BEC attacks to trick your employees or business partners into diverting funds.

Develop a BEC Response Plan

The sooner you report a BEC attack, the better your chances of recovering losses. Be sure to have a plan in place to immediately notify your bank of the fraud, make a report to IC3.gov and reach out to your local FBI field office. The plan should also include quickly engaging your IT and information security staff to determine if there has been a network or email compromise.

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

5 Tips for Payment Staff: Help Protect Your Business Against BEC Scams

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