FRAUD + CYBERSECURITY

Defending against business email compromise

WELCOME

Defending against business email compromise

Business email compromise (BEC) is a sophisticated scheme used by organized cybercrime groups. The aim is to trick your employees into sending fraudulent payments by impersonating your executives, business partners or vendors—and it's a pervasive problem.

According to the FBI Internet Crime Complaint Center (IC3), BEC fraud led to adjusted losses of nearly $2.4 billion in 2021. That's up from around $1.9 billion in losses reported a year prior.

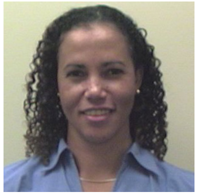
We're here to help our clients combat BEC through ongoing education, data-driven payment screening and attempted recovery of funds, among other efforts. But a comprehensive strategy to protect against BEC requires your organization to implement strong controls, train staff to follow policies and regularly test adherence to them.

Remember, it is vitally important to take any phone calls from us regarding unusual transactions very seriously. That phone call could be your last chance to avoid fraud losses!

We hope you find this guide valuable in protecting your business from BEC and raising awareness from every employee.

Alec Grant

Head of Client Fraud Prevention
Commercial Banking



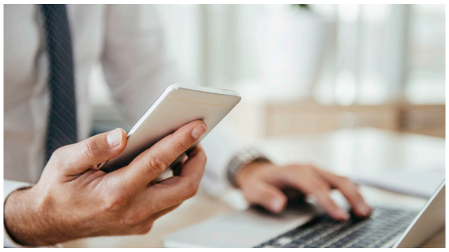
Jenifer Robinson

Head of Client Fraud Prevention
Corporate & Investment Bank

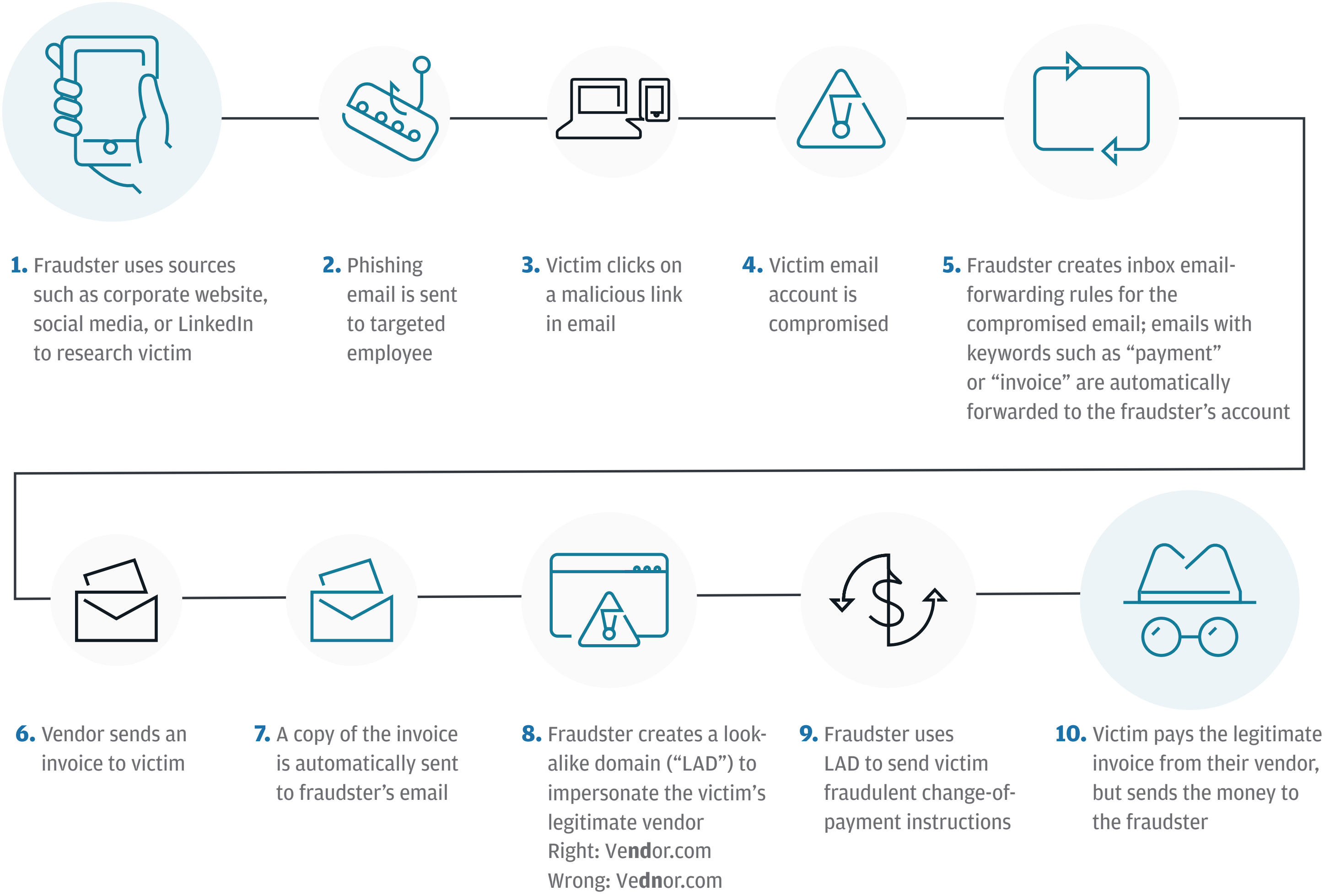
Inside these pages you will find:

Anatomy of a BEC attack

Email hacks often go unnoticed until it's too late. We broke down the anatomy of a common BEC attack to help you understand the multiple stages of fraud and how cybercriminals methodically find their targets.



Be aware, below is just one example of how a BEC attack can unfold. BEC schemes can take different forms and may not exhibit every characteristic shown here.



1. Fraudster uses sources such as corporate website, social media, or LinkedIn to research victim

2. Phishing email is sent to targeted employee

3. Victim clicks on a malicious link in email

4. Victim email account is compromised

5. Fraudster creates inbox email-forwarding rules for the compromised email; emails with keywords such as "payment" or "invoice" are automatically forwarded to the fraudster's account

6. Vendor sends an invoice to victim

7. A copy of the invoice is automatically sent to fraudster's email

8. Fraudster creates a look-alike domain ("LAD") to impersonate the victim's legitimate vendor
Right: Ve**nd**or.com
Wrong: Ve**dn**or.com

9. Fraudster uses LAD to send victim fraudulent change-of-payment instructions

10. Victim pays the legitimate invoice from their vendor, but sends the money to the fraudster

FRAUD + CYBERSECURITY

Everyone has a role in combating BEC

BEC attacks are methodic and sophisticated. The scale of this threat requires an organization to act as one in preventing fraud. That means every employee has some responsibility or part in protecting the firm.

For executives and leadership

- Recognize that BEC can present an existential risk to the business. Leadership must make BEC prevention a priority given the associated costs, downtime and reputational damages.
- Leaders have a unique role to play in establishing a culture of security in the business. They must lead by example and be vocal in raising organizational awareness and providing resources. Accountability begins and ends with them, and it's up to them to ensure that controls and programs (like employee testing) are in place at a high level.
- BEC attacks can change in shape and form. Those responsible for high-level strategy should keep up to date with emerging threat trends, as it may dictate how they defend the organization or deploy resources.

For senior and middle management

- Review email security controls, including: multifactor authentication, parameters to detect email inbox forwarding rules that send emails to external addresses, automatic labeling of all external emails and historical email logging that can be used in an investigation.
- Execute the security framework put in place by leaders. Train and test employees on a regularly established basis. Conduct phishing tests that assess whether employees can accurately identify and report suspicious emails.
- Consider hiring an external organization that can notify you when domains similar to yours are registered.

For payments staff and other treasury employees

- Adhere to policy and ensure controls are faithfully and consistently followed, particularly when performing a callback. You're the front-line defense of the organization; avoid leaving gaps for fraudsters to sneak through.
- Complete required learnings or participate in table-top exercises.
- Be judicious with what you post on social media. Cybercriminals will use profiles to research employees; avoid posting specific information about job responsibilities and projects, or personal information like streets you grew up on or pets' names.

FRAUD + CYBERSECURITY

Performing a proper callback

The importance of a validating callback cannot be stressed enough. This is the only true way to protect against BEC. However, there are multiple ways in which callbacks can go wrong, especially without formal procedures for performing callbacks.

As a ground rule, never use a phone number provided in an email. Your business should also have a set of checks that ensure a callback was performed. To help you create and enforce callback controls, here's more information on what to do and what not to do.

1 Don't rely on inbound phone calls

Always conduct an outbound call to the party to confirm they are legitimate.

Never ask that a vendor call you to validate payment instructions. **Never** use an inbound call to update contact information.

Why? Relying on inbound calls is an invitation for criminals to call you. If a fraudster has taken over a vendor's email, they'd know when you request that partner to call you. An outbound call from your staff to the party removes the risk that an employee falls prey to an enterprising criminal on the other end of the line.

2 Don't trust the number provided

Always use a known or trusted number for a system of record, and continually update any internal database for improved reference ability.

Never use a phone number provided to you in an email thread, invoice or attached documentation.

Why? Fraudsters will be all too happy to validate the transaction if you call them directly. Train staff to use this system of record repeatedly, as just one deviation from the controls opens the door to fraud.

3 Do speak with requestor

Always speak to the party who is personally accountable for the change in instructions.

Never settle for speaking with just any employee of the vendor that's initiated a payment or change.

Why? Fraudsters with email control will exploit messages between parties. Let's say your staff calls an accounting employee at the vendor, who then emails their own CFO for validation. What your staff and the vendor don't know is that cybercriminals have hacked the CFO's email and control it. This would allow fraudsters to circumvent your controls and direct the accounting employee under the presumed guise of the executive.

4 Don't assume internal controls have been followed

Always confirm controls were executed as intended and none of the above mistakes were made.

Never presume that a callback was performed.

Why? Human error happens; minimize its risk by actively ensuring procedures have been followed exactly as they were laid out.

FRAUD + CYBERSECURITY

When JPMorgan Chase calls

BEC attacks have resulted in multimillion dollar fraud losses (we have many public examples), however these losses can be prevented through controls. It requires a team effort between your organization and JPMorgan Chase to keep you from being the next victim. One way we can help your organization protect against fraud is by alerting you to any irregular transactions so we can discuss them with you.

This may be your last chance to stop fraud losses! Educate your payments staff to take our phone calls very seriously. These calls are a warning that a payment could be fraudulent.

Always perform a validating callback using a phone number from a system of record in response to any email requesting a payment, change of payment instructions or change of contact information. Never trust email alone!

If we call you about a transaction, double check that your controls have been properly executed. Do not assume a callback has been performed.

Understand that once a payment has been released, **there are no guarantees the funds will be recovered.**

Keep your contact information up to date so we can reach you promptly if needed.

Do not trust payment instructions provided from a business partner. Always validate that whoever is providing the instructions has performed a separate validating callback to the actual requestor.

Fraud protection requires being vigilant together. A successful partnership involves diligently reviewing any payments we flag and performing validating callbacks to fight back against potential fraud losses.

JPMorgan Chase continually invests in our fraud protection tools and services. Visit our **Fraud Solutions webpage** to learn more about products and solutions.