Fraud Prevention Starts Here:
Tackling Business Email Compromise

BANK OF SAN FRANCISCO

| A Growing Threat to Every Organization |

Business Email Compromise (BEC) is one of the fastest growing and most financially devastating forms of cybercrime today. Using deception, impersonation, and stolen credentials, fraudsters infiltrate legitimate business communications, often without detection, *until it's too late*.

⚠ **Once a payment is released, recovery is not guaranteed.**

BEC losses are preventable through awareness, strong internal controls, and clear communication. That's why, at Bank of San Francisco, we're committed to helping raise awareness and provide best practices to safeguard your firm against BEC.

This guide outlines:

- **How a BEC Attack Unfolds**
- **The critical roles every employee plays in prevention**
- **The right way to perform a validating callback**

Let's take a closer look at how these schemes work and best practices to safeguard against BEC.

Bank of San Francisco continually invests in our fraud protection tools and services.

Visit our Security and Fraud Center to learn more.

How a BEC Attack Unfolds

Business Email Compromise (BEC) attacks often go undetected *until it's too late*. To help you recognize the warning signs, we've broken down a typical BEC scheme, illustrating how cybercriminals methodically **identify, target,** and **exploit** their victims across multiple stages.

⚠ *Keep in mind:* This is just one example of how a BEC attack can unfold. These schemes can vary in complexity and may not follow every step 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 and email account is compromised

4. 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

5. Vendor sends an invoice to the victim. A copy of the invoice is automatically sent to the fraudster's email

6. Fraudster creates a look-a-like domain to impersonate the victim's legitimate vendor

7. Fraudster sends victim fraudulent change-of-payment instructions

8. Victim pays the legitimate invoice from their vendor but unwittingly sends the money to the fraudster

Who is responsible for defending against BEC?

| Everyone has a role in combating BEC |

Business Email Compromise (BEC) attacks are *methodical* and *sophisticated*. Every employee is a critical part of the armor in safeguarding the firm.

For Executives and Leadership

- **Understand the stakes**: BEC poses an existential risk to your business. Leadership must treat prevention as a top priority due to the potential financial loss, operational disruption, and reputational damage.
- **Lead the culture of security**: Executives have a unique responsibility to set a tone from the top. Be visible, vocal, and proactive in raising awareness, allocating resources, and embedding accountability across the organization.
- **Stay informed**: BEC tactics are constantly evolving. Those shaping company strategy must stay current on emerging threats to ensure defenses remain effective.

For Managers and Technology staff

- **Audit and strengthen controls:** Review key email security features, including:
  - Multifactor authentication (MFA)
  - Alerts for inbox forwarding rules to external addresses
  - Automatic labeling of external emails
  - Historical logging for forensic investigation
- **Put training into practice:** Conduct regular cybersecurity training and realistic phishing simulations to ensure employees recognize and report suspicious activity.
- **Monitor external risks:** Consider hiring an external organization that can notify you when domains similar to yours are registered.

For Payments Teams and Treasury Staff

- Strictly adhere to internal policies and **never skip a callback when verifying changes to payment instructions.** Fraudsters count on mistakes or shortcuts.
- **Engage in ongoing education**: Complete all required cybersecurity training and participate in tabletop exercises to simulate real-world BEC scenarios.
- **Be mindful of your online footprint**: Cybercriminals mine social media for clues. Avoid posting specific job duties, project details, or personal information (like pet names or childhood streets) that could be used in social engineering attacks.

Bottom line: BEC defense is everyone's job. With the right mindset, processes, and awareness at every level, your organization can build real resilience against these evolving threats.

| Performing a Proper Callback |

The importance of a **validating callback** cannot be overstated, it remains the **single most effective control** in preventing Business Email Compromise (BEC).

☑ **Always rely on trusted, pre-established contact information.**

Callbacks can easily **fail** if your organization lacks clear, standardized procedures. Without consistency, even well-meaning employees may fall into a fraudster's trap. To help you implement strong callback controls, here are key *dos* and *don'ts*:

🔓 1. Don't Rely on Inbound Phone Calls

☑ **DO** make an **outbound** call to the known contact to confirm payment or changes.
❌ **DON'T** request that the vendor or client *call you* to validate information.

Why? Inbound calls can be easily spoofed. If a fraudster has compromised a vendor's email, they'll know you're expecting a callback and may pose as the vendor. Making a verified outbound call to a known number eliminates this risk.

🚫 2. Don't Trust Phone Numbers Provided in Emails

☑ **DO:** Use a **system of record** to retrieve trusted contact numbers.
❌ **DON'T:** Use any phone number provided in an email thread, invoice, or attachment.

Why? Fraudsters will eagerly validate a payment when you're unknowingly calling them. *Train staff to rely only on internal records,* and update those records regularly for accuracy. Even a single exception to this control can lead to financial loss.

🕵 3. Do Speak with the Accountable Individual

☑ **DO:** Confirm changes directly with the person responsible for the payment, such as the CFO.
❌ **DON'T:** Settle for speaking with *any employee* at the vendor's company.

Why? If a fraudster has control of a vendor's executive email, they can manipulate internal communication. For example, your staff might speak to the vendor's accountant, who in turn emails their CFO for validation—only to have the fraudster (in control of the CFO's inbox) approve the fraud. Direct confirmation with the accountable individual helps close this gap.

💡 **Bottom Line:** Callbacks are only effective when they're *done properly, consistently, and according to policy.* Build a culture that reinforces this expectation, and back it up with *training, documentation, and audits*.