Keeping Your Money Safe: Business Email Compromise

Denise Owens, CFE, SVP, Fraud Department Manager

Businesses and individuals lose billions of dollars every year due to fraud. While PlainsCapital Bank has a seasoned fraud prevention team in place to protect our customers, we understand that the best protection is education. To that end, our Fraud Prevention Series, "Keeping Your Money Safe," highlights the latest fraud scams with helpful tips on how you can avoid them.

In today's business climate, employees often have more emails flooding their inbox than they can realistically pay attention to. Most of us simply scan subject lines and paragraphs to find what we need to do and quickly do it.

This environment creates a wide-open playground for cybercriminals hoping to defraud businesses. In fact, one of the most effective email frauds today exploits this exact vulnerability.

It's known as Business Email Compromise (BEC), a form of social engineering that results in more than $12.5 billion of losses worldwide, according to the Federal Bureau of Investigation. With BEC, malicious actors hack or spoof the email accounts of CEOs and other high-level executives to trick employees into making an unchecked money transfer to a fraudulent account.

How Does the Scam Work?

Most executives keep a high profile. While this is good for business, it makes them an easy target for cybercriminals. BEC scammers routinely research a company's key stakeholders, acquiring professional and personal details about them and their surrounding network, to make the scam more believable.

Once a scammer chooses their target, they'll either hack into their target's email or create a "spoof" email that looks very similar to a company's email domain. Then, they'll send emails from that inbox to find a willing victim—often a direct report or someone in the executive's network who processes payments.

Scammers will often begin a BEC email chain with a simple question like "Are you in today?" and follow up three or four more times, using information only the individual they're impersonating would know. When they've built enough credibility, the scammer will ask their victims to pay an invoice or wire money to a vendor on their behalf since they are boarding a plane, at the hospital with a family member, etc. And once a business wires money to a fraudulent account, it's notoriously difficult to recover—especially if the fraud isn't discovered quickly.

BEC is effective because it relies on the fast-paced nature of business today and the power dynamic inherent in corporate settings. Plus, the increasing number of corporate database breaches equip attackers with confidential information that makes it easy to create targeted messages.

How to Prevent Business Email Compromise

Business email compromise is so pervasive that local law enforcement agencies struggle to keep up with the caseload. Furthermore, financial institutions have limited recourse when it comes to recovering funds.

For these reasons, the best way to confront BEC is to prevent it through employee education. Corporations across the globe have implemented mandatory IT Security training to increase their employees' awareness of this particular scam.

Here are some policies you can implement in your business to avoid falling victim to malicious actors:

- **Educate key employees on common BEC techniques.** Fraudsters often use similar methods when executing a BEC scam. Implement training sessions to help employees notice the warning signs of a BEC attempt, including spoofed email addresses, requests that ask for secrecy or quick turnaround times, and appeals to correspond via personal email accounts.
- **Institute a "channel switching" policy for transactions.** Most BEC attempts work because employees fail to properly confirm a request from an executive. Implement a policy that requires employees who process payments to confirm with the requestor through a different communication channel, such as the company's instant messaging system, office phones, or a text message to the requestor's personal phone.
- **Be wary of publicizing the whereabouts of executives.** BEC attacks often occur when an executive is travelling, and finding this out isn't particularly difficult. In many cases, a quick scroll through the newsfeed of your company's social media account will tell them everything they need to know. Limit an attacker's window of opportunity by delaying social posts, omitting specific days/times on posts covering an event, and notifying select employees when an executive is traveling.
- **Implement a payment review process to identify fraud.** Recovering funds from a fraud scam like BEC is difficult. It's even more difficult if the fraud isn't discovered quickly. Implementing a payment review process that seeks to single out instances of fraud is always a good idea. Depending on your business structure, you can conduct weekly, biweekly, or monthly meetings to review invoices and wires and verify payments with relevant personnel.

Keeping Your Money Safe

When BEC works, the subsequent investigation is often difficult and, for some parties, embarrassing. While implementing a fraud education program is a great way to prevent BEC, partnering with a financial institution that takes fraud prevention seriously is paramount.

PlainsCapital Bank's Fraud Department provides educational resources for businesses and customers to help detect and prevent fraud on their accounts. For more information about our fraud prevention efforts, visit our fraud resources page.