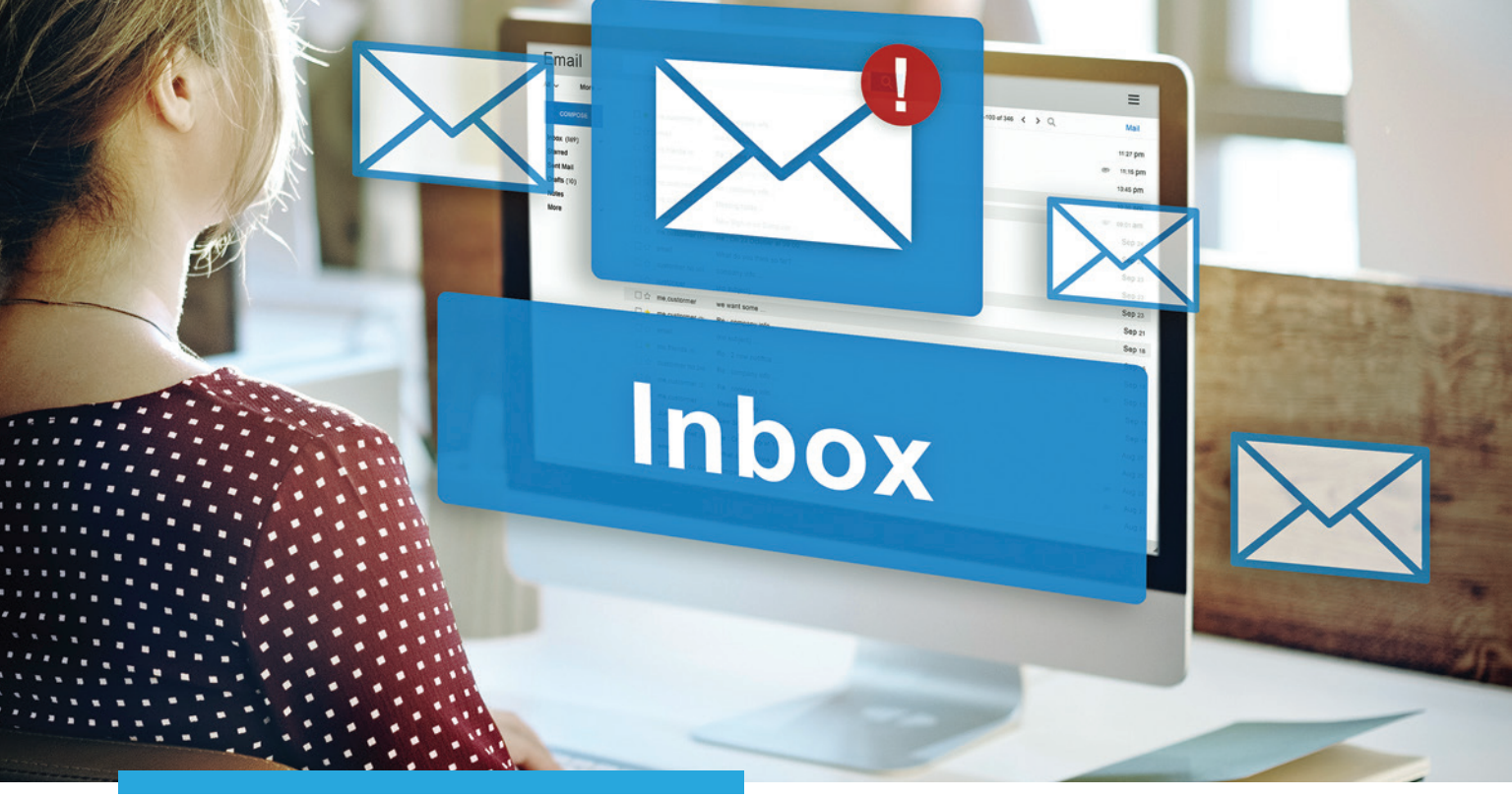

PROTECT YOUR BUSINESS FROM C-SUITE EMAIL FRAUD

Wire fraud continues to increase, and one method—**Business Email Compromise** (BEC), also known as C-suite or CEO email fraud—is becoming more popular.

What is BEC?

Criminals hack into business email systems to identify those who act on and/or authorize wire transfers. Armed with that information, the criminals then create fraudulent email wire transfer instructions posing as someone authorized to approve payment orders, like the CEO, CFO, or other executives. The fraudulent email may be sent to a person within the company who processes wire transfer requests. The employee, believing the request is legitimate, initiates the wire. The bank receives the request, uses established verification procedures (User ID, password, callbacks, etc.), and processes the wire as usual.

There are two additional fraudulent scenarios on the rise.

1) The first scenario involves the criminal taking control of a victim company's email account in order to change wire transfer instructions, directing a payment to a different bank account than what was intended. Fraudsters are clever to cover their tracks by setting up rules in the victim's email account to hide the fraudulent communications.
2) The second scenario involves the criminal posing as a trusted vendor or business partner. The criminal sends the victim company an invoice that looks legitimate but contains fraudulent payment instructions. The company, believing the vendor's email is legitimate initiates the wire.

PACIFIC WESTERN BANK

pacwest.com

Member FDIC EQUAL HOUSING LENDER

COM040719

BUSINESS EMAIL COMPROMISE

How do I protect my business?

Consider using some of these best practices to establish internal controls that work for your business:

» Execute call-back verifications for any transaction requested by email or text, regardless of the sender.
» Require dual control approvals for all wire transfer transactions.
» Set limits for employees with wire transfer authority.
» Install and maintain anti-virus, anti-spyware, and anti-malware software on all business computers. Routine maintenance should include regular, full scans for viruses, malware and the like.
» Conduct regular security awareness training with employees.
» Advise all employees to use extreme caution if asked to divulge account information or banking credentials.
» Don't deviate from existing procedures and scrutinize any exception, particularly when beneficiary payment instructions are changed.
» Be careful if posting financial or personnel information to social media or company websites, including vacation dates of executives. BEC fraud often occurs when an executive is out of the office.

How do I identify if we received a phishing email that could lead to a compromise?

» Read the entire email, then read it again. While the subject line might look fine, there could be clues in the body of the message. Does the request or introduction make sense? Is it coming from someone you know?

Would they write an email like this one?

» Does the email address look legitimate? Look closely for misspellings, dashes, dots or anything else that might not be there. Is the format correct?
» Example: Susie.smith@xyxcompany.com vs ssmith@xyzcompany.com vs Susie.smith@abccompnay.co.
» Are you the right person to receive the email? Would you normally receive this type of email?
» Are there misspellings in the email?
» Is there incorrect or improper grammar?
» Does the sender use the word "kindly"?
» Is there a link or "Click Here" button included in the email?
» Is there an attachment?
» Is the email requiring secrecy or urgency?
» Does it include a threat (e.g., to cut off service, close an account, etc.)?
» Does the web address match the business name of the sender?
» Does the sender ask for non-public personal or bank proprietary details?
» Are you being asked for computer login credentials like user name or password?
» Does the wording state they are asking for this information to help you prevent fraud?
» Is the email from someone you don't know?

What do I do if I suspect an email compromise?

» Notify the bank and law enforcement as soon as you detect the fraud. Early notification is critical, especially if funds were wired. The longer it takes to report the fraud, the less chance of recovering funds.

No business is immune to this type of fraud, and BEC schemes are becoming a larger threat to companies worldwide. Pacific Western Bank highly recommends taking preventative measures like using technology and internal controls to protect your assets. If your company has been a victim of BEC or other Internet crime, you are encouraged to file a complaint here https://www.ic3.gov/default.aspx.

Additional information can be found through the FBI Public Service Announcement at https://www.ic3.gov/media.