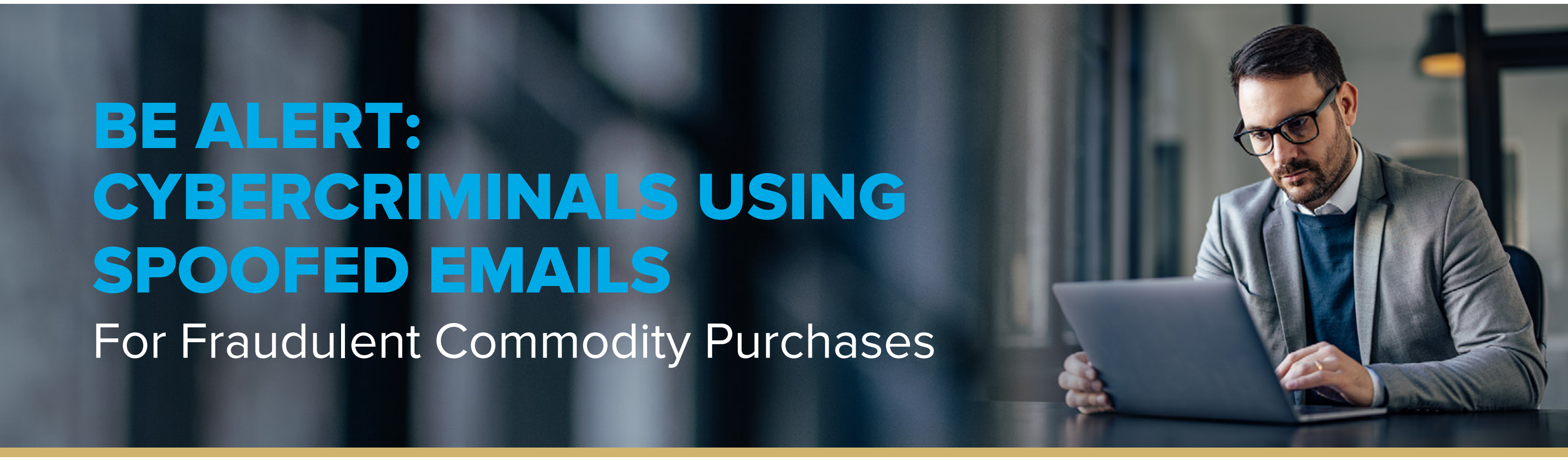
BANC OF CALIFORNIA | TOGETHER WE WIN®



BE ALERT: CYBERCRIMINALS USING SPOOFED EMAILS

For Fraudulent Commodity Purchases

The prevalence of business email compromise (BEC) scams is growing, so it is essential for businesses to stay vigilant and protect themselves from fraud. One of the more common BEC tactics that businesses face today is spoofed emails.

This type of scam involves fraudsters using fake email domains and display names to deceive vendors into believing they are carrying out legitimate business transactions. In many cases, business vendors assume they are fulfilling large purchase orders for commodities without realizing that the source of the emails was fraudulent. To help protect your business from this kind of cybercrime, it's important to understand how this common scam works and the steps to take to protect your business.

How Email Spoofing Works

Spoofed emails are a type of BEC scam in which fraudsters use fake email domain addresses as well as the display names of current or former company employees, or even fictitious names, to make it appear as if the message has come from a legitimate source when in actuality it has not. The unsuspecting vendor assumes they are conducting real business transactions fulfilling purchase orders for commodities, unaware they have become victims of a scam. Unfortunately, by the time these business vendors realize they have been deceived, it can be too late; their goods have already been shipped or their money has already been lost.

In addition, criminals may also provide fake credit references and fraudulent W-9 forms in order to establish net-30 or net-60 repayment terms that allow them to initiate additional orders without providing upfront payment, further delaying the discovery of the scam.

Protecting Your Business from Fraudulent Purchase Requests

When it comes to preventing fraud, knowledge is power—the more you know about criminal actors and their tactics, the better protected your business will be. Fortunately, there are steps you can take to protect your business and employees from fraudulent purchase requests:

- Verify the source of an email by directly calling a business's main phone line to confirm the identity and employment status of the email originator rather than calling numbers provided via email contact
- Ensure that the email domain address is associated with the business it claims to be from to avoid spoofed emails from illegitimate sources
- Do not click on any links provided in emails; instead, employees should type the URL/domain name directly into their web browser's address bar to avoid malicious phishing links designed specifically for stealing data or money from unsuspecting victims
- Ensure all outgoing payments require and receive dual approval from two different people within your organization so if one person falls victim to a scam attempt, the transaction can still be stopped before it goes through
- Train employees how to recognize phishing attempts and know what kinds of emails should be flagged for further investigation before responding or taking any action on them

BE AWARE: CYBERCRIMINALS USING SPOOFED EMAILS

For Fraudulent Commodity Purchases

Spoofed emails are an increasingly common way for scammers to target businesses around the world. As such, it is important for businesses owners, executives and employees to know how these scams work and what steps can be taken to prevent them from happening at their own establishments. By following some simple guidelines such as verifying sources before conducting any financial transactions and avoiding clicking suspicious links sent via email, you can help protect your business against this type of digital fraudulence and help keep your business safe!

For more information on protecting your business from fraud, visit the **Banc of California Business Insights** page.

To read more Business Insights articles, please visit:
bancofcal.com/business-insights

BANC OF CALIFORNIA | **TOGETHER WE WIN®**