Frost

Business Insights

Defending Against Business Email Compromise (BEC)

Business email compromise (BEC) is a sophisticated scheme used by organized cybercrime groups. The aim is to deceive you and your employees into sending fraudulent payments by impersonating your company executives, business partners or vendors.

Frost is here to help our clients combat BEC through ongoing education, data-driven payment screening and attempted recovery of funds. However, the first step is for your company to have a business plan that implements strong controls, trains staff to follow policies and regularly tests adherence to them.

The key to stopping BEC is to always follow up with an outbound call to the requester using a known and trusted phone number to verbally verify any new payment instructions. Never use a phone number provided in an email thread, invoice or attached document. Always speak to the person directly accountable for the new beneficiary account.

HOW TO IDENTITY THE DIFFERENT TYPES OF BUSINESS EMAIL COMPROMISE (BEC)

Change to Payee Account Information: A legitimate-looking email is received from a vendor, executive within your company or an employee requesting that future payments or direct deposit be sent to a new account number, usually at a different financial institution. The excuse for the change could be that their current account is under audit or no longer available, so they want to have the payment sent to a different account at another bank.

Change to Payment Method: A legitimate-looking email requesting a change in payment method. For example, one of your vendors who has always been paid by check is now requesting to have payments sent via ACH or wire transfer.

Fraudster Creates a Look-Alike Domain: Fraudsters send an email from a domain to impersonate a legitimate vendor requesting a change in payment instructions. Be sure to check that your vendor's email address is accurate. Fraudsters will often switch letters in the address to make it appear authentic, but when closely examined, is misspelled.

The best way to protect against BEC is by validating callback for every set of new payment instructions. You are your company's first line of defense, and it may be your last chance to avoid a fraud loss.

WE'RE HERE TO HELP

Scan the QR code or visit: FrostBank.com/Protect to learn more.

R(12/24)