Business Email Compromise (BEC) Red Flags

Author: eFraudPrevention

BankUnited

What to Look for in an Email

Suspicious Email Address of the Sender

The email address of the sender(s) can mimic legitimate businesses. Threat actors often leverage email addresses that resemble reputable organizations but alter or omit a few letters and numbers.

Generic Greetings and Signatures

Lack of contact information in an email signature block, or generic greetings such as “Sir/Ma’am” or “Dear Valued Customer” are strong indicators of a phishing email.

Misspelling and Layout

Odd sentence structure, misspellings, poor grammar, and inconsistent formatting are strong indicators of a potential phishing attempt.

Spoofed Websites and Hyperlinks

When hovering a cursor over links in the body of an email, if links do not match, the link may be spoofed. Malicious variations from legitimate domains leverage different spellings or domains such as .net, vs .com. Other tactics include the usage of URL shortening services to conceal the true destination of links.

Suspicious Attachments

Unsolicited emails which request users to open or download attachments are common delivery mechanisms for malware.

Common Indicators & Red Flags

- Emailed transaction instructions for direct payment to a known beneficiary; however, the beneficiary’s account information is different from what was previously used.
- Emailed transaction instructions for direct wire transfers to a foreign bank account that has been documented in customer complaints as the destination of fraudulent transactions.
- Emailed transaction instructions for direct payment to a beneficiary with which the customer has no payment history or documented business relationship, and the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the customer has historically paid.
- Emailed transaction instructions include markings, assertions, or language designating the transaction request as “Urgent,” “Secret,” or “Confidential.”
- Emailed transaction instructions are delivered in a way that would give the financial institution limited time or opportunity to confirm the authenticity of the requested transaction.
- Emailed transaction instructions originate from a customer’s employee who is a newly authorized person on the account or is an authorized person who has not previously sent wire transfer instructions.
- A customer’s employee or representative emails financial institution transaction instructions on behalf of the customer that is based exclusively on email communications originating from executives, attorneys, or their designees. However, the customer’s employee or representative indicates he/she has been unable to verify the transactions with such executives, attorneys, or designees.

- A customer emails transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.
- A wire transfer is received for credit into an account; however, the wire transfer names a beneficiary that is not the account holder of record. This may reflect instances where a victim unwittingly sends wire transfers to a new account number, provided by a criminal impersonating a known supplier/vendor while thinking the new account belongs to the known supplier/vendor, as described in the above BEC Scenario 3. This red flag may be seen by financial institutions receiving wire transfers sent by another financial institution as the result of email compromise fraud.

All content is for informational purposes only and does not constitute legal, tax, or accounting advice. You should consult your legal and tax or accounting advisors before making any financial decisions.