Servis 1st Bank Best Practices

Tips to Protect Against Business Email Compromise (BEC) Email Scams

Criminals may target you by pretending to be your CFO, CEO or a trusted contact. Below are a few best practices to help protect your organization from BEC attacks.

1. Be wary of external emails

Handle emails from outside your organization with caution, especially ones that ask you to click a link or open a document. If you do not recognize the sender or are not expecting the communication, do not click any links or open any attachments and immediately notify your IT or information security department.

2. Look closely at email addresses

Examine email addresses in the reply field to confirm they match the exact spelling of the originating company's domain and the individual's name. Fraudsters frequently use deceptive lookalike domains to trick victims. They may also use compromised email accounts, which can only be detected by performing a trusted callback to confirm the validity of the email.

3. Read emails carefully

Be suspicious of emails relating to payments or accounts that use urgent language or provides excuses for the lack of a callback option. Other common examples of BEC red flags and pressure tactics include poor grammar, punctuation, spelling and words such as "kindly send" or "kindly respond".

4. Perform a callback

Always perform a callback to the person making a request using a phone number from your records when setting up a new account, processing a request for payment, changing payment instructions or changing contact information.

Elements of a Callback

- Confirm all of the account details, including the new account number.
- Do not confirm payment instructions only via email – always perform a call back using a phone number from your records to the person making the request.
- If a callback is not currently a part of your company's payment control process, try to implement one or escalate the issue to someone who can.

5. Follow up on suspicious transactions

If you receive a call from the bank about a suspicious transaction, pay close attention to the information provided and reconfirm that your organization performed all applicable controls, including a callback. Clients often confirm payments as valid only to later report them as fraudulent.

What to Do If You Suspect Fraud

If you suspect fraud, immediately notify your ServisFirst Bank account officer.
The sooner you contact the bank, the higher the chances of getting your funds returned.

Servis 1st Bank®

For more information on how to protect your organization, please visit www.servisfirstbank.com/fraud-prevention-education/.

Please contact Cash Management with any questions at 866.922.5794 or contact your local banker.