UNDERSTANDING BUSINESS EMAIL COMPROMISE

EMAIL COMPROMISES appear as a legitimate business transaction.

Also known as Whaling, Spearing and CEO Fraud, Business Email Compromise (BEC) scams targets a business or commercial client to initiate large transfers of funds to an account the fraudster controls.

Business Email Compromise fraud targets CEOs, bookkeepers, accounts payable and other high-level employees who can authorize wire transfers.

These types of fraud do not have malicious links or attachments and can often evade traditional solutions. A reliable email security solution can flag common keywords used and allow the fraud to be recognized before it is complete.

Attackers pretend to be CEOs who request payments or lawyers who need sensitive data or information. Human resources and bookkeeping are also targeted to try and get sensitive employee data.

To protect your business, a multi-factor authentication system for all sensitive data or wire transfers is crucial. Contacting CEOs or bookkeepers to ensure it is a valid request can also reduce your odds of being a victim of scams.

STOP. **THINK. DON'T BE FOOLED.**

Notify your bank immediately if you have given out your information, so they can help protect your account.

RCBBank.com/Security
Fraud Dept. 877.361.0814

RCB BANK