Financial Education

Business email compromise (BEC)

Business email scams are on the rise as more employees are working from home. In fact, the FBI received 467,361 complaints in 2019 — nearly 1,300 every day on average — and recorded more than $3.5 billion in losses.

How to spot a BEC:

1. A fake email that appears to be from a trusted contact is sent to the employee handling payment initiation asking to send money to a new or changed bank account. Often the email appears to be from a vendor or company executive.
2. A request may ask to expedite the payment and to keep it confidential.
3. Sometimes the email may identify an outside attorney and is followed by a phone call from a person posing as an attorney.

Common characteristics of BECs include:

- Scams frequently involve a change in payment instructions or a payment to a new beneficiary and are urgent in nature.
- Businesses and personnel using open source email are the most targeted, including high-level executives.
- Scam email requests are specific to the victimized business, request funds similar to normal banking activity and mimic legitimate email requests, raising few or no suspicions. Businesses should pay extra attention to email communications from regular suppliers and vendors that may be overlooked.
- Fraudulent emails may coincide with business travel dates or dates where executives or payment approvers are unable to be reached.

Put a plan in place for a second review of outgoing payments to help protect your business from BECs.

Visit **usbank.com/bec** for more information.

usbank