Business Fraud Is Changing
VERIFY BEFORE YOU SEND



Fraudsters are finding increasingly convincing ways to impersonate banks, executives, employees, customers and vendors. Their goal is often the same: get someone inside your business to change legitimate payment instructions and send money to an account controlled by the fraudster.

The most important thing your team can remember is simple:
If payment instructions change, STOP and VERIFY before you send.

Fraud Prevention at a Glance

Before changing payment information or sending funds:

- **Verify independently.** Confirm changes to account numbers, routing numbers, payees or payment instructions using trusted contact information you already have on file.
- **Check the sender carefully.** Review the full email address for subtle misspellings, extra characters or unusual domains. Hover over the sender's email address and any links to see the true address or destination before taking action.
- **Don't click first.** Do not click links or open attachments from unknown or suspicious senders. If a message appears to come from someone you know but seems unusual, verify it through another trusted method.
- **Don't rely on email alone.** Even a legitimate email account can be compromised, allowing a fraudster to send convincing messages from someone you regularly communicate with.
- **Be cautious of urgency.** Fraudsters often pressure employees to act immediately or bypass normal procedures.
- **Protect your credentials.** BLC Community Bank will never ask for your password, token or fob code, or multi-factor authentication code.
- **Use dual approval when possible.** A second review can help catch a fraudulent change before money leaves your account.
- **Monitor activity.** Account alerts and regular transaction reviews can help identify suspicious activity quickly.

Put Your Treasury Management Tools to Work

BLC Community Bank offers fraud prevention solutions designed to help protect your business:

- **ACH Positive Pay** to help identify unauthorized ACH transactions.
- **Check Positive Pay** to help detect potentially fraudulent check activity.
- **Account Alerts** to notify you of important account activity.
- **Dual Control & Approval Workflows** to provide additional oversight for payment initiation and changes.

REMEMBER: If payment instructions change, stop and verify before you send.
A five-minute verification call can prevent a costly loss.

Questions about fraud prevention or Treasury Management solutions?

Contact BLC Community Bank at **920-788-4141** or email **TM@blccb.com**.

Read the full article at **www.blccb.com/blog/business-fraud**