



A single fake email can lead to costly fraud.



LOGANSPORT
SAVINGS BANK

Protect Your Business From Email Fraud

Understand Business Email Compromise & Fake Invoice Scams

HOW THE SCAM WORKS

RED FLAGS TO WATCH FOR

- **1 SCAMMER GAINS ACCESS**
A criminal gains access to a business email account through phishing or other means.
- **2 FAKE EMAIL OR INVOICE SENT**
The scammer pretends to be a trusted vendor, client or partner and sends a fake invoice or payment request.
- **3 PAYMENT INSTRUCTIONS CHANGE**
The email includes new ACH or wire instructions, different from ones you have used before.
- **4 PAYMENT IS SENT**
The payment is made to the fraudster's account, and the money is quickly moved, often making it difficult to recover.



Urgent or unusual requests for immediate payment



Requests coming from a new or unfamiliar email address



Unexpected attachments or links



Changes to payment instructions or bank account information



Poor grammar, spelling errors, or messages that don't match the sender's usual tone

STEPS YOU SHOULD TAKE

Always **verify** any change in payment. Use **multiple channels** to confirm requests. **Be cautious** and treat any request to change bank account information as suspicious. **Report** suspected scam attempts to your bank and do not send the payment.