A REAL-WORLD BUSINESS RISK

The Email That Could Cost Your Business

Business email compromise (BEC): when a believable message tries to redirect your money or data.

THE SCENARIO

A familiar vendor emails: “Our bank details have changed. Please send today’s payment to the new account before 4 PM.” The display name looks right. The account number does not.

FIVE CONTROLS THAT BREAK THE CHAIN

01 **STOP THE PAYMENT**

Do not process changed banking instructions based on email alone.

02 **VERIFY INDEPENDENTLY**

Call the vendor using a previously verified number, not the number in the message.

03 **CHECK THE SENDER**

Inspect the full email address and domain; familiar names can be spoofed.

04 **USE TWO APPROVERS**

Require separate review of sensitive account changes and high-risk payments.

05 **REPORT AND RESPOND**

Notify finance/security immediately; if funds moved, contact the bank promptly.

THE HUMAN-RISK LESSON

A legitimate-looking email is not proof of a legitimate payment request.

References: FBI Business Email Compromise (fbi.gov); IC3 BEC guidance (ic3.gov).