4. Business Email Compromise (BEC) / CEO Fraud

Attackers hijack or spoof an executive’s email to trick employees into making unauthorized payments.

This type of attack exploits trust in senior leadership to bypass normal verification.

WHAT IS BEC?

Attackers hijack or spoof an executive’s email to instruct employees to make payments

Scenario: Hassan Gets a Fake Vendor Payment Request

Hassan receives an email from the “CFO” saying, “Please update the vendor’s bank details to this new account.”

However, the real CFO’s email account was compromised, and the attacker is providing fraudulent bank information.

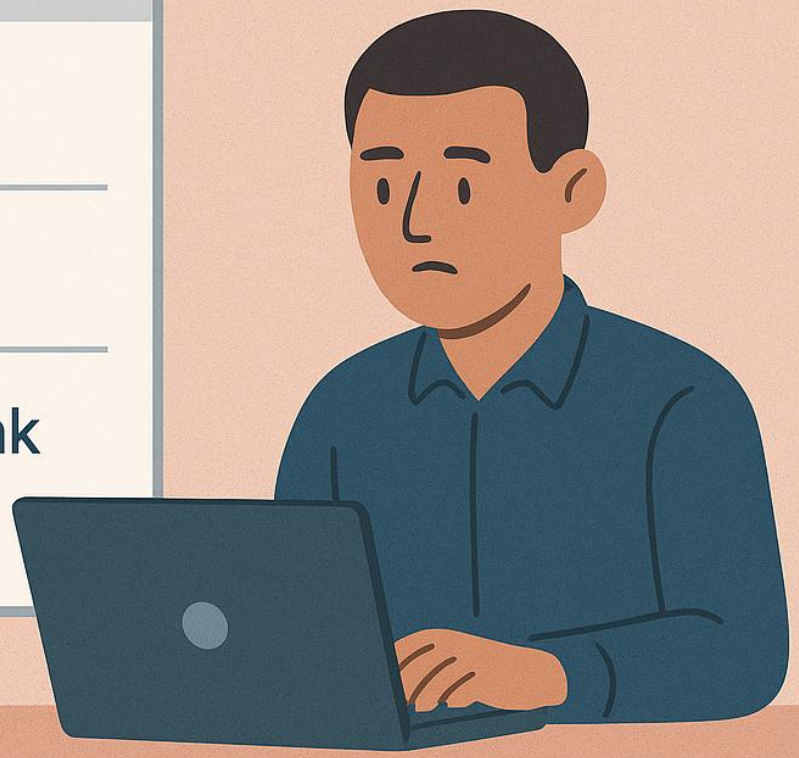
Lesson: Always confirm critical changes like bank details through an independent, verified channel before acting.

SCENARIO: HASSAN GETS A FAKE VENDOR PAYMENT REQUEST

cfo@company.com

To hassan@company.com

Please update the vendor bank details to this new account



How BEC Works?

Attackers may:

- Hijack the actual CEO mailbox
- Create lookalike domains
- Forward real email threads
- Insert fraudulent instructions

Common BEC Variants

- Fake payment updates
- Fake refund requests
- Fake salary adjustments
- Fake vendor onboarding

Defense Against BEC

- Always verify bank detail changes via **phone call**
- Implement **payment approval workflows**
- Enable MFA on all executive accounts
- Disable automatic forwarding rules