# BUSINESS EMAIL COMPROMISE

# BEC Red Flags

Know the Warning Signs. Protect Your Organization.

Business Email Compromise (BEC) is the most financially devastating form of cybercrime. Attackers impersonate executives, vendors, or partners to trick employees into wiring money, sharing sensitive data, or changing payment details. **Learn these red flags—they could save your company millions.**

## RED FLAGS — STOP AND VERIFY

### 1 Urgent Wire Transfer Request

Pressure to send money immediately, bypass normal approval, or keep the transaction secret.

*"I need you to wire $47,500 right now. I'm in a meeting and can't talk. Don't tell anyone yet."*

### 2 CEO / Executive Impersonation

Email appears to be from the CEO, CFO, or owner but uses a slightly different email address or domain.

*"From: mike.johnson@firstunderwrlters.com (note the missing 'i' in underwriters)"*

### 3 Vendor Payment Change

A known vendor suddenly requests payment to a new bank account, often citing a 'bank audit' or 'account change.'

*"Please update our banking info for future payments. Our new account details are attached."*

### 4 Unusual Tone or Language

The message doesn't match how the sender normally writes—different greeting, formality, grammar, or signature.

*"Hey, kindly do the needful and process this payment at the earliest. Regards, Michael"*

### 5 Reply-To Mismatch

The 'From' name looks legitimate but the reply-to address goes to a different, unknown domain.

*"From: CFO Name Reply-To: cfo.company@gmail.com"*

### 6 Secrecy or Pressure

Requests that you not verify through normal channels, skip approvals, or keep the transaction confidential.

*"This is highly confidential—M&A; related. Do not discuss with anyone. Just process the payment."*

### 7 Last-Minute Changes to Closing

Wire instructions change at the last moment during a real estate closing, M&A; deal, or large transaction.

*"UPDATED: Please use these new wire instructions for tomorrow's closing. The bank changed our account."*

### 8 W-2 or PII Request

Request for employee tax forms, Social Security numbers, direct deposit details, or other personal data.

*"HR: Please send me a PDF of all 2025 W-2 forms for our records review. Need it by end of day."*

## PROTECT YOURSELF — 5 CRITICAL STEPS

### 1 VERIFY BY PHONE — ALWAYS

Before wiring money, changing payment details, or sharing sensitive data, call the requester directly using a known, trusted phone number—not one from the suspicious email. This single step stops the vast majority of BEC attacks.

### 2 CHECK THE EMAIL ADDRESS CAREFULLY

Look at the full email address, not just the display name. Watch for subtle misspellings: 'rn' instead of 'm', swapped letters, extra characters, or lookalike domains (.co instead of .com, -inc instead of inc).

### 3 ENFORCE DUAL AUTHORIZATION FOR PAYMENTS

Require two people to approve any wire transfer, ACH payment, or payment detail change above a set threshold. No single person should be able to authorize and execute a large payment alone.

### 4 SLOW DOWN — URGENCY IS A WEAPON

Attackers create artificial urgency to bypass your critical thinking. If something feels rushed, unusual, or pressured—that is the red flag. Take 10 minutes to verify. A legitimate request can wait; a fraudulent one cannot.

### 5 REPORT IMMEDIATELY — SPEED SAVES MONEY

If you suspect a BEC attempt, report it immediately to IT and management—even if you're not sure. If money was wired, contact your bank within the first hour for the best chance of recovery. File an FBI IC3 report at ic3.gov.

## IF MONEY WAS SENT — ACT NOW

1. **CALL YOUR BANK IMMEDIATELY**
   Request a wire recall or payment hold. Speed is critical—funds can often be recovered within the first 24 hours.
2. **CALL YOUR IT TEAM / MSP**
   They will secure the compromised email account, check for forwarding rules, and investigate the attack vector.
3. **CALL YOUR INSURANCE BROKER**
   Contact First Underwriters at (425) 242-5357. Your cyber policy may cover financial losses from BEC and social engineering fraud.
4. **FILE AN FBI IC3 REPORT**
   Report the incident at ic3.gov. The FBI's Recovery Asset Team has recovered hundreds of millions in BEC losses.
5. **PRESERVE ALL EVIDENCE**
   Do not delete the fraudulent email. Save headers, attachments, and all related correspondence. Screenshot everything.

## BEC BY THE NUMBERS

| $55B+ | #1 | $125,000 | 70% |
|---|---|---|---|
| Total BEC losses reported to FBI (2013–2024) | Most costly cybercrime type per FBI IC3 | Average loss per BEC incident | Of BEC attacks target wire transfers |

Courtesy of **First Underwriters Insurance Brokers**
4055 Lake Washington Blvd NE, Suite 100, Kirkland, WA 98033 | **(425) 242-5357** | firstunderwriters.com
*Print and display in break rooms, near copiers, and in finance offices. For cyber insurance questions, contact your broker.*