threat level: human

The attack vector you can't patch.

Business Email Compromise

The invoice and wire-transfer fraud that costs businesses the most, and how to stop it.

$3.05B
reported BEC losses in 2025
FBI IC3, 2025

$55B+
global BEC losses, 2013 to 2023
FBI IC3, 2024

62%
of breaches involve the human element
Verizon DBIR, 2026

SPOTTING THE FRAUDULENT REQUEST

01 A change to payment details by email
New bank or wire instructions for an invoice, a vendor, or payroll.

02 A look-alike or spoofed sender
A domain off by one letter, or a display name that matches a real executive.

03 Urgency plus secrecy
A rush wire that asks you to skip the usual approval or keep it quiet.

WHERE IT HIDES

04 A hijacked email thread
A reply that continues a real conversation from a compromised mailbox.

05 Vendor and invoice fraud
A trusted supplier 'updates' their bank account just before a large payment.

ACCOUNTS AND MONEY TO PROTECT

06 Mailbox rules you did not set
Auto-forwarding or hidden inbox rules an attacker uses to watch and bury replies.

07 Gift-card and payroll diversion
Requests for gift cards, or a change to an employee's direct-deposit account.

08 Free-mail and look-alike domains
A staff or vendor 'request' from a personal address or a one-character-off domain.

DO / DON'T

DO

- Verify every bank-detail change by calling a number you already have on file.
- Require a second approver for any new or changed payment details.
- Enable MFA on all email accounts and alert on new inbox-forwarding rules.
- Confirm vendor changes with a known contact, never the email thread itself.

DON'T

- Do not trust payment instructions that arrive only by email.
- Do not use a phone number or link from the suspicious message to 'verify'.
- Do not let urgency or an executive's name skip the approval step.
- Do not release a payment before the callback is complete, even under a deadline.

THE ONE MOVE

Confirm every payment change by calling a number you already have, never one from the email, and require a second approver for new or changed bank details. A genuine vendor expects the callback.

IF IT HAPPENS

1. Call your bank immediately and request a wire recall. Speed decides recovery.
2. Reset the password and revoke sessions on any compromised mailbox, then delete rogue rules.
3. Preserve the emails and full headers for investigators.
4. Report to ic3.gov within hours, and warn affected vendors and staff.

Get a briefing like this every week, free.

threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: FBI IC3 Annual Report (2025); FBI IC3 BEC PSA (2024); Verizon DBIR (2026). Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.