Business email compromise (BEC)

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: Finance, treasury, management and IT leads.

What to do when someone impersonates an executive or a vendor to divert a payment, or when a real email account is used for that purpose. The first hours decide whether the money is recovered.

Signs it is happening

- An urgent, confidential request for a wire transfer from an executive.
- A vendor announcing by email that its bank account has changed.
- A legitimate invoice with the payment details altered.
- Replies that go to an address different from the sender's.
- A vendor claiming a payment the organization has already made.

How serious it is

Critical	The transfer has already been made.
High	An internal email account was compromised, even if nothing was paid.
Medium	An attempt detected before payment, from an external domain.

First hour

- [ ] **1.** If the transfer has already gone out, call the bank immediately and ask them to stop or reverse the transaction.
- [ ] **2.** Ask the bank in writing to contact the receiving bank to freeze the funds.
- [ ] **3.** Suspend all pending payments to that account and to that vendor.
- [ ] **4.** Confirm by phone, on a number you already know, with the real executive or vendor.
- [ ] **5.** Keep every email in the conversation without modifying it.
- [ ] **6.** If an internal mailbox is suspected, change its password and close its sessions.

Preparation (before the incident)

- Require verification through a second channel for every bank account change.
- Require dual approval for transfers above a defined amount.
- Turn on two-step verification for finance and management email.
- Automatically tag emails that come from outside the organization.

Detection and Analysis

- Determine whether the email came from a real compromised account or from a lookalike domain.
- Check the mailbox for forwarding rules, deletion rules and access from unusual locations.
- Rebuild the timeline: first contact, request, payment.
- Identify what other information the attacker saw in the mailbox.

Containment

- Block the spoofing domain in email.
- Revoke sessions and remove malicious rules from the compromised mailbox.
- Notify the vendors and customers whose email threads were tampered with.

Eradication

- Request the takedown of the lookalike domain from the registrar.
- Review the other finance and management accounts for the same rules.
- Remove third-party applications with access to the mailbox that no one recognizes.

Recovery

- Follow up daily with the bank on the recovery of the funds.
- Revalidate the bank details of all active vendors.
- Resume payments only under the strengthened verification process.

Lessons Learned

- Identify which control was missing: verification, dual signature or email protection.
- Update the payment procedure and train finance with this case.
- Evaluate insurance that covers wire transfer fraud.

Evidence to preserve

- Every email in the conversation, with headers.
- The transfer receipt and the details of the destination account.
- Access logs of the mailbox involved.
- A record of the steps taken with the bank.

What not to do

- Waiting until the next day to call the bank: every hour reduces the chance of recovering the money.
- Confirming the account change by replying to the same email.
- Deleting the fraud emails to “clean up” the mailbox.
- Treating it only as an accounting matter: there is usually a compromised account behind it.

Who to notify

- Your own bank and, through it, the receiving bank.
- Senior management and legal counsel.
- The Public Ministry (Ministerio Público), by filing a criminal complaint with receipts and emails.
- The impersonated vendor or customer.
- cert.gt, with the domain and the account used, to alert others.

When to close the incident

- The bank has confirmed the outcome of the recovery effort.
- The criminal complaint has been filed.
- No mailbox retains rules or access belonging to the attacker.
- The new payment verification control is in operation.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

General good-practice guidance; it does not replace legal or specialized technical advice for your case. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).