Business email compromise playbook

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

When to use this playbook

Use this playbook when a payment request, bank detail change or invoice looks fraudulent, when an executive or supplier email account may be controlled by someone else, or when funds may have been sent to a fraudulent account.

Before you start: prerequisites

Complete these before an incident, as part of planning.

- The finance team has a call-back procedure on a known number for any change of bank details.
- The bank's fraud and recall contact is on the contact sheet, available 24 hours.
- Mailbox rules and forwarding can be listed for any user.
- Two-step sign-in is required on email accounts, preferably with phishing-resistant methods.

Workflow

Work in this order. Record each step and its time in the incident log.

1. If a payment was sent, call the bank immediately and ask for a recall and any indemnification documents. Time matters.
2. File a complaint with the FBI IC3 (ic3.gov) as soon as possible, whatever the amount, so that it can help banks and law enforcement try to freeze funds.
3. Find the account used: check the sender, reply-to address, look-alike domains, and mailbox rules or forwarding set by an intruder.
4. Contain: reset the password, revoke sessions, remove the intruder's rules and forwarding on every affected mailbox.
5. Verify any open payment requests by phone on a known number.
6. Search for other victims inside and outside the company, and warn customers and suppliers whose details were used.
7. Preserve the emails, headers and bank records.

Decision points

Stop at each of these and record the decision, the decider and the time.

Decision	Who decides	Information needed
Recall funds or accept the loss?	Finance lead, executive sponsor	Amount, bank guidance, time since the transfer
Is personal data exposed from the mailbox?	Privacy lead	Mailbox contents and access logs

Decision	Who decides	Information needed
Tell the insurer?	Executive sponsor	Policy terms; crime and cyber cover

Notices to check

Open section 10 of the plan and confirm whether any of these start a notice clock.

- If personal information of employees or customers was in the compromised mailbox, treat it as a possible data breach.
- Insurance notice may be required for both crime and cyber policies.

Exit criteria and follow-up

Close the playbook only when all of these are true.

- Bank recall requested, and the IC3 complaint filed.
- Intruder access removed from every mailbox.
- The payment verification procedure is updated.