



Business Email Compromise

Overview

Suspected mailbox compromise, invoice diversion or executive impersonation should be treated as both a security incident and an evidence-preservation problem.

Act quickly

If a fraudulent payment may still be recoverable, contact the bank immediately and ask for the payment to be recalled or frozen where possible.

What to do now

01 Pause risky transactions

Stop or verify pending payments, bank-detail changes and unusual instructions.

02 Secure the account

Reset credentials, revoke active sessions and review multi-factor authentication.

03 Preserve mailbox evidence

Keep suspicious emails, headers, forwarding rules, sent items and deleted-item activity.

04 Check neighbouring accounts

Identify whether other users, shared mailboxes or supplier accounts may be affected.

05 Record the timeline

Note when the suspicious activity was first noticed and each containment action taken.

06 Contact financial institutions

If funds moved, notify the bank immediately and preserve payment references.



**DIGITAL
FORENSICS**

INCIDENT HELP SHEET

Business Email Compromise

What not to do

- ! Do not permanently delete suspicious emails or mailbox rules before they are documented.
- ! Do not rebuild or re-image affected systems until relevant logs and account evidence are preserved.
- ! Do not notify a suspected insider or attacker using a potentially compromised email channel.
- ! Do not assume a password change alone ends the incident; active sessions and rules may remain.

Evidence to preserve

- ✓ Suspicious emails in original format where possible
- ✓ Full email headers
- ✓ Mailbox forwarding and inbox rules
- ✓ Sign-in and audit logs
- ✓ MFA and account-recovery changes
- ✓ Payment requests, invoices and altered bank details
- ✓ Known-good examples of legitimate supplier communications

Before speaking to a forensic specialist

Keep the original device or account available, avoid unnecessary changes, write down the sequence of events while it is fresh, and explain any containment or recovery actions already taken. The more complete the context, the easier it is to assess what evidence may still be available.

Need help now?

Digital Forensics can assist with evidence preservation, forensic examination and clear reporting.

Phone: 01634 672677

Email: info@digital-forensics.co.uk

Web: digital-forensics.co.uk