



THREAT ADVISORY

Threat Advisory: Business Email Compromise Against Finance Teams

The mailbox-rule and supplier-impersonation patterns we keep finding in finance departments, with the detection logic and the four controls that stop them.

PUBLISHED

June 24, 2026

READING TIME

9 minutes

AUTHOR

SCIAT AFRICA Research

ABSTRACT

Business email compromise produces losses without malware, without an exploit, and frequently without any alert firing. This advisory describes the patterns our investigations keep surfacing in finance functions — mailbox forwarding rules, thread hijacking, supplier bank-detail changes — and the specific detections and controls that interrupt them.

Topics: Email Security · Fraud · Detection

WHAT TO TAKE AWAY

- A new mailbox forwarding or hide-from-view rule on a finance account is one of the highest-signal detections available, and most tenants do not alert on it.
- Thread hijacking defeats the “look for a suspicious sender” heuristic, because the email arrives inside a genuine conversation.
- Any change to supplier bank details must be verified out of band, on a number held on file beforehand.
- Legacy authentication protocols that bypass multi-factor authentication remain the most common initial access path.
- Payment approval thresholds should be set against what a single compromised mailbox could move.

CONTENTS

01 What the pattern looks like

02 Detections worth building this week

03 The four controls that matter most

04 If you think it has already happened

01 What the pattern looks like

A credential is phished, usually through a convincing sign-in page rather than an attachment. The attacker authenticates — often via a protocol path that does not enforce multi-factor authentication — and then does something quiet: creates an inbox rule that forwards mail matching keywords such as invoice, payment or bank to an external address, or moves those messages to an obscure folder so the legitimate user stops seeing them.

From there the attacker watches. When a real invoice thread appears, they reply inside it, from the compromised account or a lookalike domain, with amended payment details. There is no malware, no exploit, nothing for a signature to match, and the email arrives inside a conversation the recipient has been part of for weeks.

02 Detections worth building this week

The following are available in most mainstream mail platforms' audit logs and are high-signal rather than high-volume, which makes them realistic to alert on rather than merely to collect.

- Creation or modification of an inbox rule that forwards externally, or that moves mail matching payment-related keywords.
- Tenant-level or mailbox-level forwarding enabled on any finance or executive account.
- Successful authentication using a legacy protocol that bypasses multi-factor enforcement.
- Sign-in from an unusual location or autonomous system followed within minutes by a mail-rule change.
- Registration of a new multi-factor method shortly after a password reset.
- Outbound mail volume spikes from a single internal account.

03 The four controls that matter most

Phishing-resistant multi-factor authentication on all mail access, with legacy authentication protocols disabled outright — these protocols are the most common route we find for authentication that should have been blocked.

Out-of-band verification of any change to supplier payment details, by calling a number already held in the vendor master file, never a number supplied in the request. This single procedural control stops the final step of the attack regardless of how the email was obtained.

Payment approval thresholds set deliberately against single-mailbox risk, with dual authorisation above them and no emergency override that bypasses the second approver.

External-sender marking that is visible and not habituated, combined with domain-based message authentication, reporting and conformance enforcement on your own domain so lookalike and spoofed sending is harder.

04 If you think it has already happened

Preserve before you remediate. Export the mailbox audit log and the sign-in log immediately — in several platforms the default retention is short, and the evidence of rule creation is the thread that unwinds the whole incident.

Then revoke all active sessions and refresh tokens, not just the password; enumerate and remove forwarding and inbox rules across every potentially affected mailbox, not only the one you found; check for registered multi-factor methods the user does not recognise; and review any application consent grants added during the window.

If a payment has moved, contact the bank immediately — recall is time-critical and measured in hours. Then assess the data-protection position: a compromised mailbox is a personal data breach if it held personal data, which engages the notification duties in the Data Protection Act.

About this publication

This document is published by SCIAT AFRICA, a cybersecurity and digital forensics agency based in Nairobi, Kenya. It is free to read, print and circulate inside your organisation. The web edition, which carries the same content, is at <https://sciatafrica.com/research/advisory-business-email-compromise>.

It is general guidance, not legal advice and not a substitute for an assessment of your own environment. Where it refers to a law, regulation or standard, read the instrument itself before relying on it – and talk to us if you want help applying it to your estate.

SCIAT AFRICA

info@sciatafrica.com · +254 794 946633 · <https://sciatafrica.com>