P1

## PRIORITY 1 · CRITICAL SECURITY INCIDENT

Confirmed account takeover with attempted payment fraud. Triage 15 min, notify 30 min, contain 60 min, updates every 30 min.

SECURITY INCIDENT REPORT

# Finance mailbox taken over, fake payment request sent

Syarikat Contoh Sdn Bhd · Tuesday 03 November 2026 · fictional company, mock data

| FIRST ALERT | ATTACKER ACCESS | CONTAINED | CLOSED |
|---|---|---|---|
| 01:52 MYT | 14 min | 02:06 MYT | 09:40 MYT |

### What happened

On 2 November a finance executive signed in through a phishing page posing as a supplier invoice. It relayed her password and MFA approval to Microsoft and kept the session token. At 01:52 the next morning the attacker used the token from a rented server abroad, hid replies with an inbox rule, and emailed the accounts payable clerk asking for an urgent RM 186,400 payment to a new bank account. Our hub contained the account two minutes after confirming the attack. No payment was made.

### Impact

One mailbox open to the attacker for 14 minutes. The fraudulent email was quarantined unopened. No money lost. The mailbox held customer invoices, so the client's DPO assessed PDPA notification (page 3).

### Our response against the SLA

| | | |
|---|---|---|
| Triage started | 3 min | ≤ 15 min |
| Client notified | 4 min after confirmation | ≤ 30 min |
| Contained | 2 min after confirmation | ≤ 60 min |
| Notification fact sheet | 2 hrs 41 min | ≤ 3 hrs |

### Containment actions

| TIME | ACTION | AUTHORISATION | LIFTED |
|---|---|---|---|
| 02:06 | Revoke sessions, disable sign-in for farah.a, remove attacker's inbox rule | C2, C6 · no call needed | 08:55 by client IT |
| 02:07–02:19 | Quarantine the payment request and the phishing email (7 mailboxes) | C5 | Not reversed |
| 02:21 | Block phishing domain and attacker IP on firewall and DNS filter | C4 | Still in place |

SAMPLE

**P1 · CRITICAL SECURITY INCIDENT · FINANCE MAILBOX TAKEN OVER**

## Timeline

all times MYT, from SIEM, Microsoft 365 audit and call records

| TIME | EVENT | BY |
|---|---|---|
| 02 Nov 16:18 | Phishing email "Invois tertunggak / Overdue invoice" delivered to 6 finance mailboxes. Not flagged by the email gateway (domain 3 days old). | Attacker |
| 02 Nov 16:24 | farah.a signs in through the phishing page; MFA approved; session token captured. Sign-in logged from her usual Melaka IP, so no alert. | Attacker |
| 03 Nov 01:52:07 | Alert: sign-in to farah.a from a hosting-provider IP in another country, 8 hours after her last sign-in from Melaka (impossible travel). | SIEM |
| 01:52:40 | AI Enriched: IP belongs to a VPS provider; listed by 2 threat feeds for phishing-kit hosting. Sign-in used an existing token, no password or MFA prompt. | AI assistant |
| 01:53:18 | Alert: new inbox rule moving messages containing "payment", "bank" or "invoice" to RSS Feeds. | SIEM |
| 01:53:30 | AI Grouped both alerts into one case. Suggested severity P2, verdict likely malicious (high). | AI assistant |
| 01:55 | Hub analyst starts triage. | DC hub |
| 02:01 | Alert: farah.a sends email to AP clerk "URGENT: supplier bank change, pay today", RM 186,400. | SIEM |
| 02:04 | Analyst confirms account takeover with attempted payment fraud. **Declared P1.** Playbook PB-CONTOH-014 started. | DC hub |
| 02:06 | Sessions revoked, sign-in disabled, inbox rule removed (Authorisation C2, C6). | DC hub |
| 02:07 | Payment request quarantined from the AP clerk's mailbox, unopened. | DC hub |
| 02:08 | Called client IT on-call (answered). Then Head of Finance, per the matrix, to warn against any payment change requests. | DC hub |
| 02:15 | AI Mail trace: the original phishing email reached 6 mailboxes; 2 users clicked; only farah.a signed in on the phishing page. | AI assistant |
| 02:19–02:21 | Phishing email quarantined from all 6 mailboxes; domain and IP blocked (C5, C4). | DC hub |
| 02:34 | Update 1 emailed. Further updates 03:04, 03:34, 04:04, 04:34. | DC hub |
| 03:20 | Audit log review: attacker opened 9 emails, downloaded 2 attachments (customer invoices). No other mailboxes or SharePoint accessed. No forwarding to outside addresses. | DC SOC Lead |
| 04:45 | Notification fact sheet issued to the client's DPO and Head of IT. | DC SOC Lead |
| 08:55 | Client IT reset password, re-registered MFA on a new method, re-enabled sign-in. | Client IT |
| 09:40 | Case closed as contained. Enhanced monitoring on farah.a and the 6 recipients for 7 days. | DC SOC Lead |

SAMPLE

P1 · CRITICAL SECURITY INCIDENT · FINANCE MAILBOX TAKEN OVER

## AI-assisted investigation suggestions reviewed by the SOC Lead

AI **Enrichment.** Attacker IP is on a VPS provider used by phishing kits; the session ID at 01:52 matched the one issued at 16:24 on 2 November, so the token was stolen then, not a new password guess. No MFA prompt was logged at 01:52.

AI **Scope.** No other hits for the attacker IP, phishing domain or bank account number across all logs. The AI only read logs; analysts took every action.

### Ranked causes of initial access

| RANK | SUGGESTED CAUSE | EVIDENCE | AI CONFIDENCE | ANALYST FINDING |
|---|---|---|---|---|
| 1 | Adversary-in-the-middle phishing, session token stolen | Same session ID at 16:24 and 01:52; phishing link clicked at 16:23 | High | **Confirmed** |
| 2 | MFA fatigue | No repeated MFA prompts in the log | Low | Ruled out |

## Notification

The attacker opened invoices with names, addresses and amounts owed for 37 customers. Fact sheet DC-SOC-NFS-2026-011 (04:45) gave the DPO what happened, when, what was affected and what we did. **The client decides whether to notify the PDP Commissioner and affected customers, and submits any notification.** On 4 November the DPO recorded the decision and its reasons in the client's breach register.

## Follow-up actions

| # | ACTION | OWNER | DUE | STATUS |
|---|---|---|---|---|
| A1 | Require a compliant, company-managed device for finance staff signing in to Microsoft 365 (conditional access), which blocks stolen-token reuse from other machines | Client IT | 20 Nov 2026 | Open |
| A2 | Move finance and admin users to phishing-resistant MFA (passkeys or security keys) | Client IT | 31 Dec 2026 | Open |
| A3 | Raise the severity of any sign-in from a hosting provider to a finance account straight to P2 | Dunia Canggih SOC | 06 Nov 2026 | Done |
| A4 | Introduce a call-back check on a known number before any supplier bank change is paid | Client Head of Finance | 13 Nov 2026 | Open |
| A5 | Short phishing briefing for the finance team using this incident | Client HR + DC SDM | 13 Nov 2026 | Scheduled |

**Prepared by**
Daniel T., SOC Lead
05 Nov 2026

**Reviewed by**
Hafiz R., Service Delivery Manager
05 Nov 2026

AI-assisted: alert grouping, enrichment, mail trace, scope search, ranked causes and the timeline draft, all reviewed by the SOC Lead. Issued as a locked PDF within 3 working days of closing. Editing is disabled; printing and copying text are allowed. This sample uses a fictional company, fictional people and mock data.

SAMPLE