HorseInsure Pty Ltd
Level 12, 45 Pitt Street, Sydney NSW 2000

ABN 41 209 837 156

SECURITY INCIDENT REPORT

Report Reference	INC-2025-003
Incident Type	Phishing Attack - Email
Severity Level	HIGH
Date Detected	15 March 2025, 09:35 AM
Report Date	15 March 2025
Reporting Officer	David Chen, CIO/CISO
Systems Affected	Email gateway, Microsoft 365, Claims department workstations

INCIDENT DESCRIPTION

A targeted phishing campaign was detected on 15 March 2025 targeting HorseInsure staff, specifically personnel in the Claims department. The malicious email appeared to be from an external claims management system (ClaimTech Pty Ltd) requesting urgent password verification due to "system maintenance". The email contained a link to a fraudulent login page designed to capture user credentials. Email gateway filtering initially allowed the message to pass through (sophisticated spoofing of legitimate domain). Alert triggered at 09:35 AM when multiple users from Claims department attempted to access the fraudulent page from company networks.

DETECTION AND INITIAL RESPONSE

How Detected: Email security gateway detected multiple failed authentication attempts from claims department. Marcus Lee (IT Security Analyst) reviewed logs and identified suspicious login page access attempts.

Time to Detect: Approximately 25 minutes from first user click

Immediate Actions Taken:

• 09:35 AM: Email gateway alert triggered • 09:40 AM: Marcus Lee initiated incident response protocol • 09:45 AM: Email message quarantined and removed from all user mailboxes (4,847 recipients across organisation) • 10:00 AM: David Chen notified, incident classified as HIGH severity • 10:15 AM: All affected users (3 who clicked link, 1 who entered partial credentials) identified and notified • 10:30 AM: Forced password reset issued for affected users • 10:45 AM: Email security rules updated to block similar phishing attempts • 11:00 AM: Company-wide email alert sent warning users of phishing attack

AFFECTED PARTIES AND IMPACT

Affected System	Impact Level	Details
Microsoft 365 / Email	Medium	4,847 users received malicious email; 23 users opened email
Claims Department Users	High	3 staff clicked fraudulent link; 1 staff member entered username (not password)
EquiClaim System	Low	No direct compromise; however claims data could have been at risk if credentia
Company Reputation	Medium	Risk of customer notification if data accessed; incident reported to ASIC (consid

CONTAINMENT AND REMEDIATION

Short-term Actions (Completed):

• Email quarantine and user notification: 15 March 2025, 11:00 AM • Forced password resets for 4 affected users: 15 March 2025, 10:30 AM • Email security rule updates to block sender domain variations: 15 March 2025, 11:30 AM • Claims department phishing awareness reminder: 15 March 2025, 2:00 PM • Review of email gateway filtering rules: 16 March 2025

Medium-term Actions (In Progress/Planned):

• Security awareness training refresh for Claims department: Scheduled for 22 March 2025 • Email authentication enhancement (SPF/DKIM/DMARC review): To be completed by 31 March 2025 • Phishing simulation campaign targeting Claims staff: April 2025 • Review and enhancement of user authentication controls for EquiClaim system: April-May 2025

ROOT CAUSE ANALYSIS

Primary Causes:

1. **Sophisticated phishing technique:** Email used trusted external vendor name (ClaimTech) and urgent messaging tone ('system maintenance') to bypass user caution 2. **Email gateway false negative:** Security gateway filtering rules did not initially flag the email due to sophisticated domain spoofing. The fraudulent domain was registered recently and had not been added to threat intelligence feeds. 3. **User security awareness gap:** Some users were not sufficiently cautious about verifying sender authenticity before clicking links. This reflects need for enhanced phishing awareness training. 4. **Lack of multi-factor authentication on EquiClaim:** EquiClaim system relies on username/password authentication only. MFA would have prevented compromise even if credentials were captured.

Contributing Factors:

• Claims department frequency of system communication makes them vulnerable to social engineering • Recent organisational changes to claims systems (new integrations with external partners) created legitimate sender variation • User password policies do not enforce strong passwords universally across all systems

LESSONS LEARNED AND RECOMMENDATIONS

Key Learnings:

1. Current email security filtering is effective at detecting malicious patterns but can be circumvented by sophisticated domain spoofing 2. User awareness training is critical frontline defence; approximately 5% of recipients (23 of 4,847) still clicked suspicious links 3. Rapid incident response was effective; containment occurred within 25 minutes of detection, limiting damage 4. Need for MFA implementation extends beyond IT systems to business-critical applications like claims systems

Recommendations for Prevention:

1. Implement multi-factor authentication (MFA) for EquiClaim system access (PRIORITY) 2. Deploy advanced email authentication (DMARC enforcement) to prevent domain spoofing 3. Implement email banner alerts for messages from external domains 4. Conduct department-specific phishing awareness training (Claims quarterly, others annually) 5. Establish dedicated phishing reporting mechanism with immediate response protocol 6. Consider deploying sandbox email analysis tool for advanced threat detection 7. Implement mandatory password complexity requirements across all systems

REGULATORY NOTIFICATION AND COMPLIANCE

ASIC Reportability Assessment: This incident meets criteria for reporting to ASIC as potential breach of customer data protection obligations (Corporations Act s912D). No customer data was confirmed compromised; however, risk was present.

Status: Incident reported to ASIC on 20 March 2025 as notifiable data security event. No customer notification required (no confirmed compromise).

Breach Register Entry: Recorded in HorseInsure Security Breach Register (ref: BR-2025-003)

REPORT APPROVAL

Reported by: David Chen, CIO/CISO
Report Date: 15 March 2025

Reviewed by: Angela Torres, Compliance Manager
Review Date: 17 March 2025

Approved by: Margaret Thornton, Chief Executive Officer
Approval Date: 18 March 2025