Incident Report Case 2025-05-22 Phishing Data Breach

Incident Title: Data Breach Investigation (Attempted Exfiltration)
Date: 2025-05-22
Reported by: Astor Mydz - Finance Department
Investigated by: Luis Gutierrez - SOC Team
Current State: Resolved

---

1. Summary

At 08:16 UTC the Finance user (User@Gmail.com) reported suspicious outbound bank transfer notifications. Correlated alerts indicated an attempted exfiltration via a phishing-originated credential-harvesting page. Immediate containment actions (full password reset and domain/IP blocking) were performed; as a result, no credentials were confirmed compromised.

---

2. Incident Description

- Initial report: user reported receiving a phishing email from `Malicious@Domain.com` and subsequent unusual transaction alerts.
- Detection: multiple high-value transaction alerts and simultaneous outbound flows triggered SIEM correlation rules.
- Scope: the phishing landing page attempted to harvest employee credentials and initiate fund transfers. The attempt reached multiple recipients but was interrupted by rapid containment.

---

3. Investigation and Findings

- Phishing domain: redirected to a malicious domain hosted on a foreign server (recently registered).
- Threat intel: VirusTotal and internal TI flagged the phishing domain as malicious.
- Credential status: No verified credential exfiltration was observed after forced password resets; no unauthorized persistent access found.

- Indicators (simulation/sample):
  - Suspicious IP (sample): `192.xxx.x.xx`
  - Sample file hash (placeholder): `d41d8cd98f00b204e9800998ecf8427e`

---

4. Actions Taken

1. Performed company-wide forced password reset for affected accounts.
2. Blocked malicious domain and associated IP addresses at perimeter and email gateways.
3. Isolated and imaged affected workstation(s) for forensic preservation.
4. Updated firewall and proxy rules to block similar patterns.
5. Notified impacted users and Finance leadership; coordinated with banking partner(s) to review transactions.
6. Executed short-awareness briefing for employees on identifying phishing indicators.

---

5. Lessons Learned / Recommendations

- Implement and enforce simulated phishing campaigns quarterly to reinforce detection and reporting behaviours.
- Enforce Multi-Factor Authentication (MFA) for all accounts with access to financial systems.
- Improve email gateway filtering with behavior-based/AI detection to catch newly registered malicious domains.
- Formalize an incident runbook for suspected financial exfiltration that includes immediate password resets, banking contact procedures, and forensic imaging steps.
- Encourage users to verify high-impact requests through a secondary channel before taking action.

✅ 6. Conclusion

A coordinated SOC response and immediate defensive actions prevented credential compromise and financial loss. The incident underscores the need for stronger proactive email defenses, MFA enforcement, and continuous user training to reduce phishing success rates.