Incident Response Playbook: Email and Social Engineering Attacks

Team AnubisX

Version 1.0
October 2025

Document Control

Attribute	Value
Version	1.0
Status	Draft / Operational
Owner	AnubisX Security Team
Review Cycle	Quarterly or after major incident
Approver	SOC Manager / Head of IR

Contents

1 Introduction

1.1 Purpose

This playbook defines the procedures for detecting, triaging, containing, and remediating incidents in the **Email and Social Engineering Attacks** category. It is intended for SOC analysts, incident responders, IT operations, Identity/Access teams, Legal/Compliance and leadership. The goal is to minimize credential compromise, financial fraud, and malware delivery via email or social manipulation.

1.2 Scope

Applies to organizational email platforms (Exchange/Office365, Google Workspace), webmail, mail gateways, mail clients, identity providers (Azure AD/Okta), web proxies, endpoint EDR, and business units (finance, HR, execs) targeted by social engineering.

2 Overview of the Category

Email and social engineering attacks focus on manipulating people to take actions that reduce security (disclose credentials, approve transactions, run attachments, or change configurations). Modern campaigns range from mass phishing to highly targeted BEC and OAuth consent phishing.

2.1 Common Attack Vectors

- Malicious attachments (Office macros, weaponized PDFs, ISO/IMG lures).
- Credential harvesting sites (fake IdP pages, OAuth consent scams).
- URL-based drive-by downloads and web delivery of payloads.
- Business Email Compromise (CEO/vendor impersonation, invoice tampering).
- Mailbox rule abuse / auto-forwarding to attacker-controlled addresses.
- Social engineering channels outside email (vishing, smishing) used to validate emails or bypass controls.

2.2 Primary Risks & Business Impact

- Account takeover (leading to lateral movement and data theft).
- Financial fraud (unauthorized wire transfers).
- Deployment of malware/ransomware via attachments or clicked links.
- Exposure of sensitive emails and attachments through forwarding or API abuse.
- Reputational/legal/regulatory consequences from leaked or altered communications.

3 Severity Level Assessment & MTTD / MTTR

Level	Description / Criteria	MTTD Goal	MTTR Target
Critical	Successful BEC causing financial loss, or compromise of highly privileged accounts (domain admin, cloud owner), or mass credential theft enabling widespread access.	$\leq$ 30 min	Containment within 4 hrs; recovery staged within 24-72 hrs
High	Multiple mailbox compromises, confirmed credential reuse across services, or targeted spear-phishing to executives with high impact.	$\leq$ 1 hr	24-72 hrs
Medium	Single user credential capture or malware delivery to single host without lateral spread.	$\leq$ 2 hrs	12-48 hrs
Low	Blocked phishing attempt or suspicious email reported with no compromise.	$\leq$ 4 hrs	Monitor (24-72 hrs)

Table 1: Severity Matrix - Email and Social Engineering

4 Tools & Preparation (Recommended)

- **Email Security Gateway:** Microsoft Defender for Office 365, Proofpoint, Mimecast — URL detonation, attachment sandboxing, spoofing protections.
- **Identity Protection:** Azure AD Identity Protection, Okta Risk-Based rules, conditional access policies, mandated MFA for privileged groups.
- **SIEM / Logging:** Collect mail gateway logs, mailbox audit logs, IdP sign-in logs, EDR telemetry, web proxy logs, and DLP events.
- **EDR:** For endpoint containment, live response, collection of process trees and memory.
- **DLP:** Prevent sensitive data exfil and detect suspicious uploads or forwarding.
- **User Awareness and Simulation Platforms:** Phishing simulation, targeted training for high-risk roles (Finance, HR, Execs).
- **Playbook Resources:** IR contact list, legal/regulatory contacts, finance/treasury escalation path.

5 Incident Response Phases

5.1 Phase 1: Preparation

- Implement and enforce SPF, DKIM, DMARC with quarantine/reject as appropriate.
- Configure Safe Links / URL rewriting and attachment detonation policies.
- Create easy-reporting mechanisms (Report Phish add-in) and automatic ingestion into SIEM/ticketing.

- Configure IdP risk policies: block legacy auth, enforce MFA, conditional access based on location/device risk.
- Run periodic phishing exercises and targeted awareness training.

5.2 Phase 2: Identification & Analysis

Goal: Confirm compromise, determine scope, and identify user actions.

- Triage user reports and gateway detections; examine full message headers (Received chain, SPF/DKIM/DMARC results).
- Inspect embedded URLs and attachments in sandbox; extract host/IP, path, and payload hash.
- Query IdP sign-in logs for unusual authentication patterns (impossible travel, new device, suspicious IP).
- Check mailbox audit logs for new inbox rules, send-as, forward-to addresses, or mailbox delegation.
- Leverage EDR to identify post-click activity (process creation, scripts, network connections).

5.3 Phase 3: Containment

- Quarantine or delete malicious emails across the organization via gateway actions.
- Revoke active sessions and refresh tokens for affected accounts; force password reset and re-enroll MFA if credential compromise suspected.
- Remove malicious mailbox rules and block mail forwarding to external addresses.
- Block malicious domains/IPs at DNS/proxy/firewall; add to enterprise blocklists and sinkhole if necessary.
- Temporarily elevate monitoring on business-critical mailboxes (Finance, HR, Execs).

5.4 Phase 4: Eradication

- Remove delivered payloads from endpoints; if persistence or lateral movement suspected, reimage affected hosts.
- Revoke and rotate credentials, service principals, and any tokens discovered in memory or logs.
- Disable compromised OAuth apps and revoke suspicious app permissions.
- Harden mail flow rules, update gateway detection signatures and YARA/Sigma rules for observed payloads/URLs.

5.5 Phase 5: Recovery

- Restore normal operations for remediated accounts after verification and monitoring window.
- Reconcile any suspicious financial transactions with treasury and, if needed, initiate incident-specific financial controls (stop/recall).
- Monitor affected systems and accounts closely for at least 30 days (increased logging and alert thresholds).

5.6 Phase 6: Post-Incident Activities

- Full timeline and root cause analysis; identify gaps in controls and communication.
- Update routing for DMARC (move from quarantine to reject after tuning) and refine ATP detonation rules.
- Push new detection content (SIEM queries, Sigma rules), and share IOCs with partners/threat intel.
- Conduct lessons-learned sessions and adjust phishing simulation content to mimic the attack used.

6 MITRE ATT&CK Framework Mapping

Email & Social Engineering ATT&CK Mapping

- **Initial Access**
  - T1566 — Phishing (Spearphishing Link / Attachment / Service)
- **Credential Access**
  - T1110 — Brute Force / Credential Stuffing (when used post-phish)
  - T1556 — Modify Authentication Process (OAuth abuse)
- **Defense Evasion / Persistence**
  - T1078 — Valid Accounts (mailbox takeover)
  - T1098 — Account Manipulation (inbox rules, forwarding)
- **Impact**
  - T1499 — Data Manipulation (financial fraud through BEC)

7 Key Telemetry & Logs to Collect

- Mail gateway logs (submission/transport/delivery), attachment detonation results, URL click logs.
- Mailbox audit logs (New-InboxRule, Add-MailboxPermission, Send-As).
- IdP Sign-in and Conditional Access logs (failed/successful logins, device info, risk detections).
- Proxy and DNS logs for clicked URLs and C2 connections.
- EDR process trees and memory artifacts for post-click payloads.
- DLP alerts and cloud-object access logs for potential exfil via mail/cloud uploads.

8 Subcategory Scenarios (Realistic)

Note: Scenarios are operational SOC narratives — detection, investigation steps, containment actions, eradication, recovery and lessons learned.

Scenario A: Phishing Email Attack — Credential Harvesting via Fake IdP (Spearphish)

Summary: A targeted spear-phish to Sales contains a customized message referencing a current customer opportunity and includes a link that leads to a convincingly rendered fake Okta login page. Two users entered credentials; one account was reused to access the CRM and download sensitive opportunity documents.

Detection:

- IdP: impossible travel and concurrent session alerts for a Sales user.
- Mail gateway: URL click logs showing POST to 'okta-login[.]example-malicious.com'.
- EDR: after credential use, the CRM integration user agent made API calls from an unfamiliar source IP.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* due to credential misuse and sensitive data access. IR ticket opened; Finance/Legal notified as data owner engaged.
2. **Containment:** Revoked sessions and refresh tokens for impacted accounts; forced password reset and MFA re-enrollment; removed malicious inbox rules and disabled any OAuth tokens issued to unknown apps.
3. **Forensic collection:** Pulled mailbox header and message body, sandboxed the URL, collected gateway click logs and extracted the attacker's hosting IP and TLS certificate details for intel.
4. **Hunt:** Searched IdP logs for other sign-ins from same IP/TLS cert and scanned CRM access logs for unusual downloads.
5. **Block & Mitigate:** Blocked the phishing domain at DNS/proxy and added URL to gateway blocklist; deployed a targeted ATP detonation rule to catch similar links.

Eradication:

- Removed any attacker-issued OAuth consents and revoked suspicious API keys.
- Cleaned affected endpoints if evidence of post-click payloads; reimaged hosts if persistence detected.
- Deployed detection rules (Sigma) for the fake login redirect chain and the attacker's UA/TLS cert fingerprint.

Recovery:

- Restored legitimate access to CRM after validation and monitored the accounts for anomalous activity for 30 days.
- Notified affected partners/customers if their data was accessed and coordinated with Legal/-Compliance for any reporting obligations.

Outcome & Lessons:

- Rapid detection via IdP risk signals minimized exposure; however, user training gaps were identified — introduced targeted simulated phishes to Sales.
- Tightened conditional access policies (block legacy auth, require trusted devices) and enforced risk-based step-up authentication.
- Tuned gateway detection to strip known credential harvesting redirection patterns.

Scenario B: Business Email Compromise (BEC) — Vendor Payment Fraud

Summary: An attacker impersonates a trusted vendor using a lookalike domain and sends an urgent invoice to Finance requesting a change in bank account details. A junior finance clerk prepares a payment. The fraud is caught because the clerk asked for OOB vendor confirmation per policy (random spot-check), triggering the discovery.

Detection:

- Mail gateway: sender domain similar to legitimate vendor but failing DMARC alignment; message flagged as suspicious by anti-spoofing detection.
- User report: finance clerk raised suspicion following out-of-band check.
- SIEM: discovery of the spoofed domain and its associated IP in inbound logs.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* due to potential financial loss. IR Finance teams convened; payment on hold.
2. **Containment:** Quarantined the suspicious email and removed any auto-forwarding rules from the recipient mailbox; blocked the spoofed domain at DNS/proxy.
3. **Verification:** Performed out-of-band vendor verification (phone to pre-validated vendor number) confirming the vendor details were unchanged.
4. **Forensic actions:** Collected headers, message source, and noted the spoofing method (display-name spoof vs actual domain impersonation), and raised an abuse report with domain registrar if appropriate.

Eradication:

- Blocked the lookalike domain at enterprise perimeter and added Sender Policy/Block lists in mail gateway.
- Rolled out additional rules to flag payment-related emails with bank detail changes for manual dual-approval.
- Implemented stricter vendor payment verification process and mandatory two-person authorization for wire transfers above threshold.

Recovery:

- Payment was halted and no funds were transferred.
- Conducted targeted training for finance team and added simulated BEC scenarios in phishing exercises.
- Audited other recent vendor change requests for similar patterns or malicious domains.

Outcome & Lessons:

- The combination of user suspicion and a handbook OOB verification process prevented financial loss.
- Strengthened controls: mandatory vendor verification checklist, enforced DKIM/DMARC policies, and finance workflow changes to require dual authorization.
- Added specialized detections for vendor domain lookalikes and anomalous invoice attachments.

A Appendix A — Useful SIEM / Investigation Queries

Find mailbox forwarding rules (Office365 / Azure):

```
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) -
    RecordType ExchangeItem |
Where-Object {$_.Operations -match "New-InboxRule|Set-Mailbox" } |
Select CreationDate, UserIds, Operations, AuditData
```

Splunk: detect clicks to rare domains (proxy logs):

```
index=proxy (url_host!="our-corp-domains.com")
| stats count by url_host
| where count < 10
| sort by count asc
```

Sentinel: IdP impossible travel detection (example):

```
SigninLogs
| where ResultType == 0
| extend timeDiff = datetime_diff('minute', TimeGenerated, prev(TimeGenerated))
| where timeDiff < 15 and Location != prev(Location)
```

B Appendix B — Artifact Locations & Forensic Hints

- Email headers and MIME parts (preserve raw message) — Exchange/Office365 message trace and Journal logs.
- Mailbox audit logs (forwarding rules, send-as, add-mailboxpermission).
- Gateway detonation results and sandbox artifacts (attachments and extracted payloads).
- Web proxy logs and DNS resolution logs for clicked URLs.
- IdP sign-in and token activity (refresh token usage, app consent events).

C Appendix C — Incident Report Template (Summary)

- Incident ID, detection timestamp, severity, summary of impact.
- Affected assets/accounts, list of indicators (URLs, domains, hashes).
- Actions taken (containment, eradication, recovery) with timestamps and owners.
- Root cause analysis and recommended remediations.
- Notifications performed (internal/external) and regulatory considerations.