

Phishing triage template (L1)

1. Ticket Header

- Case ID:
- Date/Time Opened:
- Assignee:
- Reported via: (User, SIEM Alert)
- Priority: (Low/Med/High/Critical)
- Status: (New/In-progress/Closed)

2. Initial risk assessment

- User-summary:
- Email received time:
- User interaction:
 - ☐ No interaction
 - ☐ Opened email
 - ☐ Clicked link
 - ☐ Opened attachment
 - ☐ Entered credentials
 - ☐ Allowed content
 - ☐ Replied/engaged sender
- Current user impact:
 - ☐ None/Unknown
 - ☐ Suspicious login prompts
 - ☐ MFA prompts
 - ☐ Account lockout
 - ☐ New inbox mail

☐ Device behaving oddly

3. Email details

- Subject:
- From (display):
- From (address):
- Reply-To:
- To/CC:
- Message-ID:
- Originating IP:
- Links:
- Attachments: (name, type, hash)

4. Indicators of Phishing

- ☐ URL is shortened/mismatched
 - ☐ Urgency/threat/reward language
 - ☐ Credential harvest attempt
 - ☐ Risky attachment types
 - ☐ External sender spoofing internal person/team
 - ☐ Same email reported previously/by multiple users
- Exposure
 - ☐ Single user
 - ☐ Multiple users
 - ☐ VIP/ sensitive components
 - ☐ Credentials entered
 - ☐ Attachment executed
- Initial severity:
 - Low: clear spam, no interaction

- Medium: link/attachment present, no evidence of interaction
- High: link/attachment opened, multiple recipients OR convincing impersonation
- Critical: credentials entered, confirmed compromise, payment diversion attempt

5. Escalation triggers (immediate)

- ☐ Credentials entered/OAuth consent granted
- ☐ Suspicious mailbox rules/forwarding
- ☐ MFA fatigue/abnormal MFA prompts
- ☐ Malware detonation positive/EDR alert present
- ☐ VIP targeted or multiple users affected
- ☐ Confirmed account compromise

6. Enrichment & analysis

a. URL analysis

- URL:
- Domain:
- Resolved IP:
- Reputation Checks:
- Redirect chain:
- Phish kit/login page:
- Screenshot/evidence captured: (Yes/No)

b. Attachment analysis

- Filename:
- Type:
- Hash (SHA256):
- Detonation/sandbox result:

- Macro/script indicators:
- AV/EDR verdict:

c. Header analysis notes

- Display name (spoofing):
- return-path (mismatch):
- received path (anomalies):
- Internal relay signs:
- SPF:
- DKIM:
- DMARC:

7. User & Endpoint Checks

a. Identity/account checks

- Recent sign-ins:
 - Unusual country/impossible travel
 - unfamiliar device
 - failed logons/ password spray indicators
- MFA prompts: (normal/abnormal)
- Mailbox rules: (none/suspicious)
- Sign-in risk/alerts:

b. Endpoint checks (if link clicked/attachment opened)

- Host:
- User logged in:
- EDR alerts present:
- Processes spawned:
- Network connections:
- Downloads created:

8. Containment actions

- Email Containment
 - ☐ Quarantined message
 - ☐ Deleted from mailboxes
 - ☐ Blocked sender/domain
 - ☐ Blocked URLs
 - ☐ Added indicators to allow/block lists
- User/account containment
 - ☐ Forced password reset
 - ☐ Revoked sessions/tokens
 - ☐ MFA re-registered
 - ☐ Disabled account (if compromised)
 - ☐ Removed malicious inbox rules/forwarding
- Endpoint containment
 - ☐ Isolated host in EDR
 - ☐ Collected triage packages/logs
 - ☐ Full scan initiated
 - ☐ Escalated to IR for imaging
- Notes (commands, timestamps, evidence links):

9. Communication (internal/user)

- ☐ User Contacted
- ☐ Guidance given
- ☐ Stakeholders notified
- ☐ Templated response used

Time of notification:

10. Outcome & classification

- Verdict: (Malicious / Benign / Spam / Suspicious-Unknown)
- Type:
 - ☐ Credential harvest
 - ☐ Malware delivery
 - ☐ BEC/invoice fraud
 - ☐ OAuth consent
 - ☐ MFA fatigue
 - ☐ Other:
- Root cause:
- Scope:
- Lessons learned/tuning opportunities:

11. Closure checklist

Evidence Captured

- ☐ EML saved
- ☐ Full headers saved
- ☐ URLs captured (original and redirected)
- ☐ screenshot(s)
- ☐ Hashes recorded (SHA256)

Follow ups

- ☐ Indicators shared with detection team
- ☐ User confirmed safe
- ☐ Follow-up monitoring set
- Closed by/time: