1. Investigation Steps

The investigation procedure follows the incident response lifecycle, which emphasizes defense and recovery from attacks. The process encompasses preparation for possible incidents, detection and analysis of threats, and restoration of affected systems.
Log actions for a mock incident:

Time Stamp	Action
2025-11-05 16:29:05	Isolated affected user's device from the network.
2025-11-05 16:46:20	Suspicious login session terminated on the mail server.
2025-11-05 17:07:10	Collected memory dump from the isolated device for forensic analysis using velociraptor.
2025-11-05 17:35:32	No mail forwarding rules were created on the compromised user account.

2. Phishing Checklist

A phishing response checklist was documented in Google Docs to minimize human error and ensure a consistent, repeatable workflow for handling complex or high-security tasks.

Initial Assessment

- Confirm email headers.
- Check link reputation via VirusTotal/URLScan.
- Check file hash via VirusTotal.
- Identify affected users.

Containment & Eradication

- Force password reset for compromised users.
- Block malicious IP at firewall.
- Delete malicious emails from inboxes.

Post-Incident

- Notify affected users and security awareness.
- Incident Response Report.

3. Post-Mortem

A post-incident review assesses a real or staged security event to uncover its root cause and measure the effectiveness of the response. It captures key takeaways from the exercise.

Simulated Event:
A phishing attack resulted in limited data exposure after the affected system was not isolated promptly.

Lesson Learned: Delayed endpoint isolation enabled unauthorized access to sensitive information. This highlighted the need to verify network-segmentation controls. The main procedural enhancement is to enable automated host isolation through a SOAR-driven workflow.

Incident Response Template

1. Executive Summary

Incident Title / Name: Phishing Incident
Date & Time Detected: 05/11/2025
Reported By / Detection Source: User
Analyst Assigned: SOC Analyst
Incident Category: Phishing
Severity Level: High

2. Timeline

Date / Time Event Description
10:19:40 UTC: Phishing email delivered to the user account
10:28:12 UTC: User clicked the link and enters credentials.
10:35:02 UTC: SIEM alert triggers on suspicious login from external source.
10:39:10 UTC: Account disabled by SOC Analyst.

3. Impact Analysis

The issue was limited to a single user account. Although credentials were compromised, containment was achieved before any lateral movement or data loss took place. Financial impact remained minimal.

4. Remediation steps

- The affected user account was secured by locking it and issuing a new password.
- The suspicious external IP address was blocked at the firewall.
- The endpoint was remediated and validated to ensure no remaining malware indicators.

5. Lessons Learned & Recommendations

A positive alert for suspicious login activity was successfully triggered and operated effectively.

Improvement required: Company-wide awareness must be created so all employees understand malicious links and their potential impact.

Prevention measure: Implementing Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) is mandatory to prevent future credential compromises from phishing.