WorkFlow

1. Preparation Phase

Tools: Google Docs, Draw.io

2. Create the Incident Response Template (SANS Format)

Create a New Doc

Title: **"Phishing Incident – Response"**

- **Executive Summary**
  - Provide a brief overview of the phishing incident, affected users, and high-level actions taken.
- **Timeline**
- **Impact Analysis**
  - Number of users affected
  - Systems compromised
  - Data access attempted/exfiltrated
  - Business impact
- **Remediation Steps**
  - Actions performed to contain the incident
  - Recovery measures
  - Verification steps
- **Lessons Learned**
  - Gaps identified
  - Process improvements
  - Recommendations

3. Document Investigation Steps

Add the Log Table

Workflow Steps:

1. Record every action as soon as it happens.
2. Maintain exact timestamps.
3. Add evidence links (screenshots, logs, header files).
4. Review and finalize after the incident is resolved.

4. Create a Phishing Response Checklist

Checklist Template:

- Confirm email headers
- Check link reputation in VirusTotal
- Identify affected users
- Validate login patterns for affected accounts
- Block sender/domain/IP at mail gateway
- Reset credentials and enforce MFA if necessary
- Document Indicators of Compromise (IOCs)
- Produce final IR report

5. Draw.io Diagram Creation

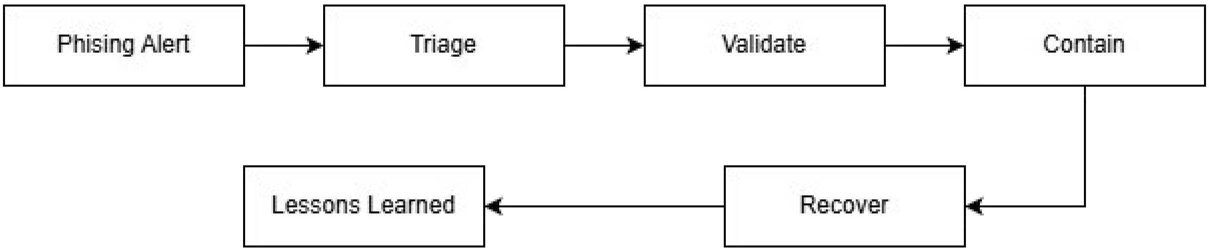

Image 1: Workflow Diagram