Investigating Phishing E-mails

How SOC L1 Analyst Investigates Phishing Emails

1. Email Header Check -

Extract and review the email header to verify:

- **Sender domain.**
- **Mail server path (Received chain).**
- **SPF, DKIM, DMARC authentication results.**

2. Link & URL Inspection -

Without clicking:

- **Hover over URLs.**
- **Extract them safely.**
- **Analyze using tools like VirusTotal, URLScan, ANY.RUN.**
- **Check if the domain is suspicious, newly registered, or impersonating a brand.**

3. Attachment Analysis -

- **If an attachment exists:**
- **Upload to sandbox (ANY.RUN, Joe Sandbox)**
- **Identify malware behavior (script execution, outbound connections)**

4. Sender Reputation Check -

Use tools to validate:

- **Domain age**
- **WHOIS information**
- **Blacklist status**
- **Email service provider used**

5. User Impact Assessment -

- **Confirm whether the user:**
- **Clicked the link**
- **Entered credentials**
- **Downloaded anything**

6. Take Action -

Depending on findings:

- **Block malicious domain/IP/URL**
- **Quarantine emails in the environment**
- **Force password reset if needed**
- **Update SIEM with indicators (IOCs)**

7. Documents & Reports -

Create a short incident note:

- **What was found**
- **Evidence (headers, URLs, sandbox results)**
- **Steps taken**
- **Recommendations for the user**