

Email Phishing Analysis

“When a suspicious email is reported to the security team, what analysis would you perform as a SOC Analyst?”

Investigation workflow:

1. Sender and Domain Analysis

Verify the Sender's Email ID and Domain

Check the domain reputation using tools like:

- ◆ VirusTotal -used to check a url
- ◆ MXToolbox - used to check a header
- ◆ AbuseIPDB - Check the ip reputations

Analyze domain details:

- 📌 Registration date
- 📌 Owner information

2. Subject Line Analysis

Examine the subject line to determine the email's intent:

- 📌 Phishing
- 📌 Social engineering
- 📌 Promotional content

3. Email Body Analysis

Look for Indicators of Compromise (IOCs) such as:

- ▲ Urgency Tactics:

Example: "Reset your account within an hour, or it will be disabled."

- 🔗 Phishing URLs:

Embedded links (e.g., behind an "unsubscribe" button) designed to mislead users

-  URL Reputation Check:

Always use trusted tools to assess link safety

👉 Attachments:

Analyze suspicious attachments in a sandbox environment

⚠️ Avoid uploading files to public tools like VirusTotal to prevent tipping off attackers

📧 4. Email Header Analysis

Obtain the email header from the message properties

Perform a header analysis:

🔧 Use MXToolbox

Select "Header Analysis"

Paste the header and generate a detailed report

Verify SPF, DKIM, and DMARC statuses

✅ 5. SPF, DKIM, and DMARC Verification

◆ SPF (Sender Policy Framework)

Checks if sending IPs are authorized

Alignment: Passes if "From" field matches "Return-Path"

Authentication: Passes if IP is authorized

◆ DKIM (DomainKeys Identified Mail)

Uses digital signatures to ensure email integrity

Alignment: Passes if DKIM domain matches "From"

Authentication: Fails if DKIM signature is invalid

◆ DMARC (Domain-based Message Authentication, Reporting & Conformance)


Built on SPF & DKIM

Policies:

- ✔ None: Email is delivered
- ✔ Quarantine: Goes to spam
- ✔ Reject: Dropped completely

🔧 6. Mail Gateway Analysis

Review key fields such as:

 From, To, Return-Path, Subject Line, Message ID

Identify how many users received the same email

Export email metadata for documentation


7. Reporting and Mitigation

Document your findings:

Analysis details

IOCs (Indicators of Compromise)

Share the results with the relevant teams and Raise a requested to :

 Block the malicious email, domain, IP address, and file hash via coordination with Network/IT/Admin teams