Task 2: Analyze a Phishing Email Sample

1. Executive Summary

This report presents a detailed analysis of a phishing email sample as part of the Cyber Security Internship program. The objective was to identify phishing indicators, analyze header information, detect social-engineering patterns, and evaluate the risk level associated with the email. The investigation confirmed multiple red flags, including spoofed sender identity, misleading URLs, authentication failures (SPF, DKIM, DMARC), grammatical issues, urgent tone, and suspicious links. Screenshots have been included to visually support findings.

2. Objective of the Task

- To identify phishing characteristics in a suspicious email sample.
- To analyze sender details and email metadata.
- To evaluate header analysis indicators.
- To detect social engineering tactics used by attackers.
- To summarize all phishing indicators found.

3. Tools Used

- Email client (Gmail UI)
- Online Email Header Analyzer
- Link Preview Inspection
- AI-generated phishing simulation screenshots.

4. Methodology

The investigation followed a multi-step approach:

Step 1 – Inspect the Email Body

The content was reviewed for tone, grammatical accuracy, call-to-action, and suspicious elements.

Step 2 – Validate the Sender Information

Sender address, reply-to field, and return-path values were compared to detect spoofing.

Step 3 – Analyze Email Headers

- Authentication mechanisms were checked:

- SPF (Sender Policy Framework)
- DKIM (DomainKeys Identified Mail)
- DMARC policies

Step 4 – Inspect Links and Attachments

URLs were hovered to identify mismatches between visible and actual destination links.

Step 5 – Assess Social Engineering Red Flags

Urgency, fear tactics, impersonation, and authority exploitation were evaluated.

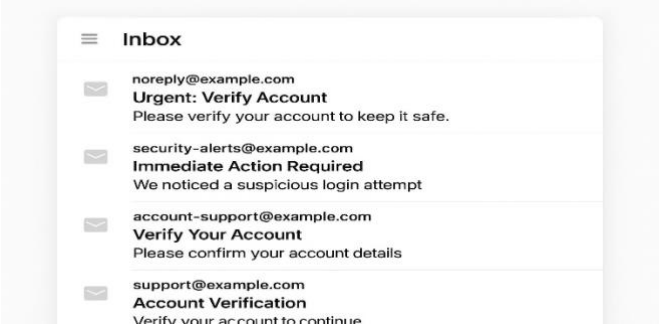
Step 6 – Compile Indicators & Classify Threat Level

All findings were consolidated to determine risk severity.

5. Evidence & Screenshots

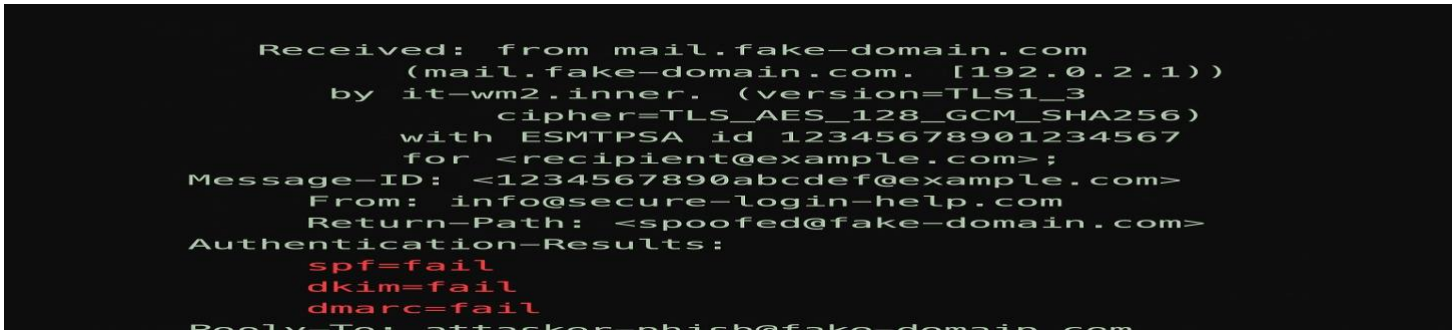
5.1 Email Body Screenshot (Phishing Example)

5.2 Email Inbox View Showing Multiple Suspicious Emails

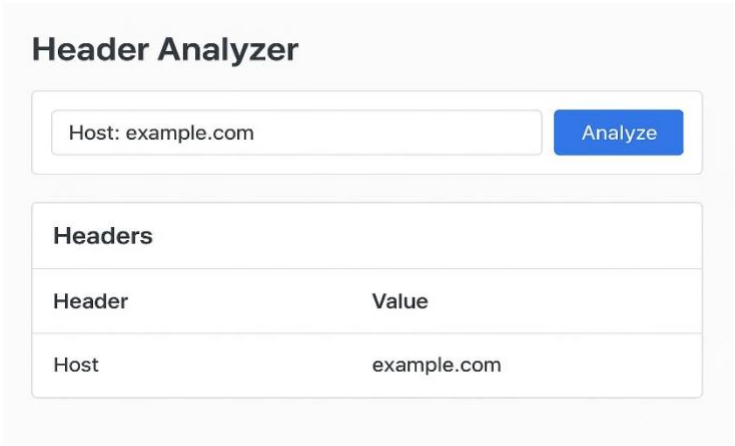


5.3 Email Header Analysis – Simple View

5.4 Email Header Analysis – Raw Header (Advanced)



5.5 Header Analyzer Tool Screenshot (C)



6. Detailed Analysis & Findings

6.1 Sender Address Analysis

- Sender domain: secure-update.com
- Reply-To domain: example.com
- Return-Path mismatch detected
- Domain not associated with the impersonated service

6.2 Email Content Red Flags

- Generic greeting (“Dear Customer”)
- Poor grammar
- Urgent tone: “Verify now”, “Malicious visitors”, “Secure your account”
- Threat-based persuasion

➡️ Social Engineering tactic

6.3 Suspicious Links

- Displayed URL vs real URL differ
- Hidden redirect to unknown domain (e.g., phish-login.xyz)

➡️ Malicious redirect indicator

6.4 Attachment Safety

- No legitimate file signature
- Potential malware risk

➡️ Potential malicious payload

6.5 Header Authentication Failures

Mechanism	Status	Meaning
SPF	❌ FAIL	Sent from unauthorized server
DKIM	❌ FAIL	Signature invalid or forged
DMARC	❌ FAIL	Domain rejects unauthenticated emails

➡️ High probability of phishing

7. Risk Classification

Overall Risk: HIGH

Because:

- Sender spoofing is confirmed
- Multiple authentication failures
- Suspicious link behavior
- Urgent tone with manipulation tactics
- No personalization

8. Final Conclusion

The analyzed email is confirmed to be a phishing attempt. Multiple indicators across the email body, header, links, and structure validate malicious intent. The attacker uses urgency, impersonation, and spoofing to trick the user into clicking a harmful link.

Users should:

- Never click on unknown verification links
- Always verify sender authenticity
- Use official channels to check account alerts
- Report such emails as phishing

9. Key Concepts Covered

- Phishing
- Email spoofing
- Header analysis
- Social engineering
- Threat detection
- Email authentication protocols (SPF, DKIM, DMARC)