Complete SOC Project Report

Project Title

Manual Phishing Email Investigation (Header & URL Analysis)

Author

Gourab Das

Target Role

SOC Analyst – Tier 1 / Junior SOC Analyst

---

1. Executive Summary

This project documents a complete end-to-end phishing email investigation performed from a SOC analyst perspective. The objective was to analyze a suspicious email, validate authentication results (SPF/DKIM/DMARC), extract and investigate malicious indicators (URLs/domains), and produce a professional SOC-style incident report.

Although the email successfully passed SPF, DKIM, and DMARC checks, further analysis confirmed phishing characteristics based on content, domain impersonation, and malicious intent. This highlights why **email authentication alone is not sufficient** to stop phishing attacks.

Final Verdict: Malicious – Phishing (Credential Harvesting)

---

2. Scope & Objectives

Scope

- Analyze a suspicious email provided in `.eml` format
- Perform header analysis
- Extract and analyze URLs
- Conduct domain reputation analysis
- Document findings in SOC-standard format

Objectives

- Understand why authenticated emails can still be malicious
- Practice real-world SOC phishing triage workflow
- Produce interview-ready project documentation

---

3. Tools & Environment

Category	Tools Used
Email Analysis	Manual `.eml` inspection, email header parsing
URL Analysis	URLScan.io, VirusTotal (reference)
Domain Analysis	WHOIS lookup, DNS inspection
Documentation	Markdown (.md) files

---

4. Email Overview

Email Metadata

- **Subject:** URGENT: Microsoft Account Will Be Disabled in 2 Hours
- **Sender Display Name:** Microsoft Technical Support
- **Sender Domain:** Look-alike domain (not official Microsoft)
- **Email Type:** HTML phishing email

Initial Red Flags

- Urgency and fear-based language
- Account suspension threat
- Short response deadline
- Embedded verification link
- Impersonation of Microsoft branding

---

5. Email Header Analysis

Header vs Body Identification

In a raw `.eml` file:

- **Header Section:** Starts at the top and ends at the first blank line
- **Body Section:** Begins immediately after the blank line

Key Header Fields Analyzed

Header Field	Observation
From	Spoofed display name, non-Microsoft domain
Return-Path	Matches sending domain (not Microsoft)
Received	External mail infrastructure
SPF	Pass
DKIM	Pass
DMARC	Pass

Why SPF/DKIM/DMARC Passed

- The attacker controlled the sending domain
- SPF validates sending server, not brand legitimacy
- DKIM validates message integrity, not intent
- DMARC only enforces alignment, not trust

Conclusion: Authentication success ≠ legitimate email

---

6. Content Analysis

Social Engineering Techniques Identified

- **Urgency:** “Disabled in 2 hours”
- **Fear:** Permanent data loss
- **Authority Abuse:** Microsoft impersonation
- **User Action Pressure:** Immediate verification

Grammar & Style Issues

- Slight grammatical inconsistencies
- Generic greeting (“Dear User”)
- Automated message disclaimer

These characteristics align with common phishing templates.

---

7. URL Extraction & Analysis

Extracted URL

- **Obfuscated Format:** hxxp://micros0ft-tech-support[.]example/verify

URL Characteristics

- Look-alike domain using character substitution (`0` instead of `o`)
- Brand impersonation
- No association with official Microsoft domains

---

8. URLScan Results

Observations

- Domain recently registered
- No historical reputation
- Page behavior indicates credential harvesting intent
- Visual similarity to Microsoft login page

Risk Indicators

- Newly created domain
- Brand impersonation
- Login form present
- External hosting provider

---

9. Domain Analysis

WHOIS Findings

- **Registration Age:** Very recent
- **Registrar:** Low-cost registrar
- **Registrant Details:** Privacy protected

DNS Analysis

- No MX records for legitimate email use
- Hosting IP associated with multiple suspicious domains

Domain Verdict

High-risk domain commonly associated with phishing campaigns.

---

10. Indicators of Compromise (IOCs)

Domains

- micros0ft-tech-support.example

URLs

- hxxp://micros0ft-tech-support[.]example/verify

Email Attributes

- Microsoft impersonation
- Credential harvesting attempt

---

11. MITRE ATT&CK Mapping

Tactic	Technique
Initial Access	Phishing (T1566)
Credential Access	Credential Harvesting (T1056)
Social Engineering	User Execution

---

12. Impact Assessment

If successful, the attack could lead to:

- Microsoft account compromise
- Unauthorized access to Outlook and OneDrive
- Data theft
- Potential lateral movement

---

13. Remediation & Recommendations

Immediate Actions

- Block sender domain
- Block malicious URL at email gateway
- Alert affected users

Preventive Controls

- User phishing awareness training
- Advanced URL reputation filtering
- Brand impersonation detection
- MFA enforcement

---

14. Final Verdict

Classification: Phishing Email

Severity: High

Confidence Level: High

This investigation confirms that the email is a malicious phishing attempt despite passing SPF, DKIM, and DMARC checks.

---

15. Conclusion

This project demonstrates a realistic SOC phishing investigation and highlights the importance of layered email security. Authentication mechanisms validate infrastructure authenticity, not sender trustworthiness. Content analysis, URL inspection, and domain reputation remain critical for phishing detection.