Phishing Email Analysis Report

Author: Chetan Mahendra
Date: 22 October 2025

1. Objective

To identify and analyze key phishing indicators in a suspicious email using both header and content inspection techniques.

2. Sample Email (Phishing Example)

Subject: "Your account will be suspended! Verify now to avoid termination!"
From: support@micros0ft-security.com
To: user@example.com
Body:
Dear User,
Your Microsoft account has been flagged for unusual activity.
Please verify your account immediately to avoid permanent suspension.
Click here to verify: https://microsoft-security-update.com/login
Regards,
Microsoft Support Team
Attachment: Account_Verification.docx

3. Analysis and Findings

Aspect	Observation	Phishing Indicator
Sender Email	support@micros0ft-security.com	Domain spoofing – 'micros0ft' uses digit '0' instead of 'o'.
Header Analysis	SPF/DKIM/DMARC failed	Indicates sender not verified; likely forged.
Links	Redirects to http://phishingsite.xyz/login	URL mismatch from official domain.
Language	Urgent and threatening tone	Psychological manipulation.
Attachments	.docx file with macros	Risk of malware infection.
Grammar/Spelling	Minor errors	Poor grammar typical of phishing.
Design/Layout	Low-res fake Microsoft logo	Fake branding – visual deception.

4. Summary of Phishing Traits Found

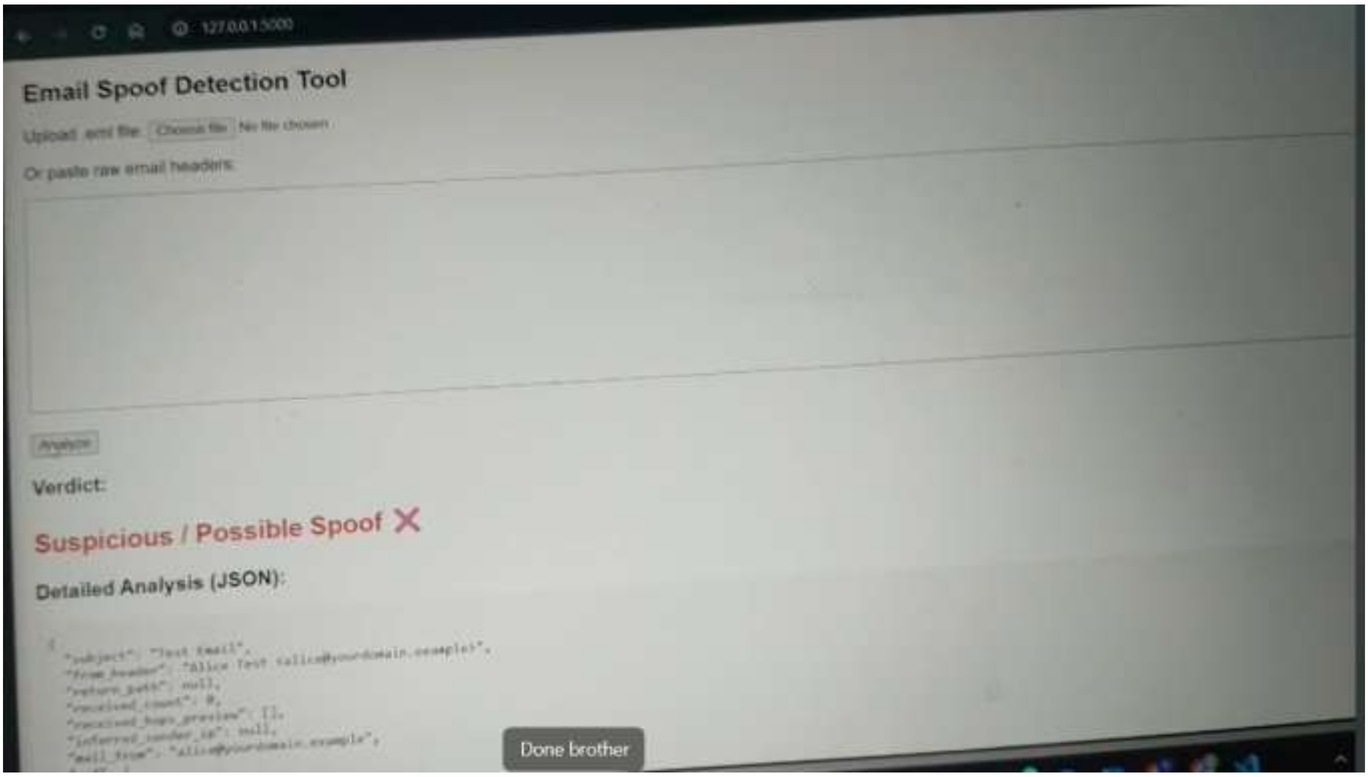
- Domain spoofing through deceptive address.
- Failed authentication headers (SPF/DKIM).
- Suspicious URLs and mismatched links.
- Urgent and threatening tone.
- Unsafe attachment with possible malware.
- Spelling and formatting inconsistencies.

5. Conclusion

The analyzed email clearly exhibits multiple phishing indicators including spoofed domain, failed authentication, malicious link, and social engineering tactics. Such emails are designed to trick recipients into revealing credentials or installing malware. Recommendation: Do not click links or open attachments. Report to IT/security team or mark as spam/phishing.

6. Screenshot (Placeholder)

Attach screenshot of email header analysis here (e.g., phishing_header_analysis.png).



Email Spoof Detection Tool

Upload .eml file: Choose file No file chosen

Or paste raw email headers:

Verdict:

Suspicious / Possible Spoof ❌

Detailed Analysis (JSON):

```
{
  "subject": "Test Email",
  "from_header": "Alice Test <alice@yourdomain.example>",
  "return_path": null,
  "received_count": 0,
  "received_hops_preview": [],
  "inferred_sender_ip": null,
  "mail_from": "alice@yourdomain.example",
```