**PHISHING EMAIL ANALYSIS REPORT**

**Objective:** Identify Phishing characteristics in a suspicious email sample.

**Sample Email Summary:**

**Subject:** "Your account has been suspended – Urgent Action Required"  
**Sender:** support@micros0ft-secure.com  
**Date:** August 3, 2025  
**Email Body Summary:**  
The email claimed that the recipient's Microsoft account had been suspended due to suspicious activity. It urged immediate action and provided a link to "verify your identity."

**Tools Used**:

Email Header Analyzer (https://mxtoolbox.com/EmailHeaders.aspx)

Web URL Expander / Link Unshortener

VirusTotal (for link/attachment scan)

Manual inspection

**Identified Phishing Indicators:**

| **Indicator Type** | **Description** |
| --- | --- |
| Sender Spoofing | The email appeared to come from Microsoft but used a domain micros0ft-secure.com (notice the use of 0 instead of o). |
| Suspicious Link | Hovering over the link showed a mismatched URL (http://verify-now-login.microsecure123.tk). This domain is not affiliated with Microsoft. |
| Urgent Language | The email used threatening language like “Your account will be permanently suspended in 24 hours.” |
| Spelling & Grammar Errors | Phrases like “verify you’re account” and “click here to continue immediately” were present. |
| No Personalization | The email addressed the recipient as “Dear User” instead of using their actual name. |
| Unusual Time | The email was sent at 3:47 AM, an uncommon time for legitimate customer support communication. |
| Email Header Red Flags | SPF failed, indicating sender was not authorized. "Return-path" did not match the sender address. |

**Header Analysis Summary**:

SPF**:** Fail

DKIM**:** Not signed

Return Path**:** [noreply@otherdomain.ru](mailto:noreply@otherdomain.ru)

**Conclusion:**

This email displays multiple red flags characteristic of phishing attempts, including spoofed sender addresses, mismatched links, grammatical errors, urgency tactics, and header anomalies.

**Recommended Actions:**

1. Do **not** click on any links or download attachments.

2. Report the email to your email provider (e.g., Outlook: Report Phishing).

3.Block the sender.

4. Educate users about checking URLs and using email header analysers.