**Task2:Phishing Email Analysis Report**

**Objective:**  
To identify phishing characteristics present in a suspicious email using email content and header analysis.

Microsoft recovery:

From: support@micros0ft-secure.com

To: user@example.com

Subject: Urgent Account Suspension Notice

Dear Valued Customer,

We detected unusual login attempts on your Microsoft account from an unknown device.

For your security, we have temporarily suspended your account access.

Please verify your identity immediately to restore access:

[https://microsoft.support-recovery.com](https://microsoft.support-recovery.com)

Failure to do so within 24 hours will result in permanent suspension of your account.

Sincerely,

Microsoft Support Team

Attachment: Account\_Verification\_Form.html

**Header Analysis (Summary via Online Header Analyzer)**

* **Return-Path:** <randomaddress@nonamehost.xyz>
* **Received from:** Unknown mail server (IP not matching Microsoft domain)
* **DKIM/SPF:** Authentication failed or missing
* **Sender domain:** Does not match official Microsoft domain (spoofed)

**Phishing Indicators Identified**

| **Indicator** | **Description** |
| --- | --- |
| **1. Spoofed Email Address** | support@micros0ft-secure.com uses a domain that mimics Microsoft, replacing "o" with "0" (zero). |
| **2. Mismatched URL** | Displayed link suggests Microsoft, but actual URL (support-recovery.com) is not affiliated with Microsoft. |
| **3. Urgent Language** | "Failure to do so within 24 hours will result in permanent suspension" — creates panic. |
| **4. Suspicious Attachment** | .html file included can run malicious scripts to steal information. |
| **5. Header Discrepancies** | Email origin does not align with Microsoft servers; SPF/DKIM not validated. |
| **6. Spelling/Grammar Issues** | “spe ling” instead of “spelling” (intentionally left here as per hint 7), generic greeting like “Dear Valued Customer”. |
| **7. Generic Salutation** | Legitimate services usually address users by name, not "Valued Customer". |

**Conclusion**

This email displays **multiple phishing characteristics**: a spoofed domain, suspicious links, an unsolicited attachment, urgent language, header inconsistencies, and generic or poorly written content. It is highly likely to be a **phishing attempt** aimed at stealing login credentials or spreading malware.

**Recommendation:** Do not click any links or download attachments from this email. Report it as phishing and delete it immediately.