**Phishing Email Analysis Report**

**Objective:** Identify phishing characteristics in a suspicious email.

* Sample mail

From: account-security@micr0soft-support.com

Subject: Urgent: Your Account Will Be Locked!

Date: August 5, 2025

To: yourname@example.com

Dear User,

We noticed unusual sign-in activity in your Microsoft account.

Your account will be suspended within 24 hours if no action is taken.

To prevent suspension, please verify your account by clicking the link below:

https://micr0soft-support.com/verify?user=yourname@example.com

Thank you,

Microsoft Account Team

## **Analysis & Phishing Indicators**

### **1. Suspicious Sender Email Address**

* **Shown Address:** account-security@micr0soft-support.com
* **Issue:** Domain uses typo-squatting (micr0soft instead of microsoft). Spoofed to look like a legitimate Microsoft address.
* **Phishing Trait:** Domain spoofing/impersonation.

### 2. **Header Analysis**

* **Tool Used:** mxtoolbox Email Header Analyzer
* **Findings:**
  + SPF/DKIM failed or not aligned
  + IP address does not match Microsoft's official servers
* **Phishing Trait:** Mismatched mail servers / header spoofing

### 3. **Suspicious URL**

* **Displayed:** https://micr0soft-support.com/verify?user=yourname@example.com
* **Real URL:** On hover, same — but domain is fake.
* **Phishing Trait:** URL mismatch / deceptive domain

### 4. **Urgent or Threatening Language**

* **Text Used:**
  + “Your account will be suspended within 24 hours”
  + “Urgent” in subject line
* **Phishing Trait:** Creates fear to prompt immediate action.

### 5. **Grammar/Spelling Errors**

* **Review:** No major errors in this case, but tone and structure are generic and not brand-specific.
* **Phishing Trait:** Subtle inconsistency, but not a strong indicator here

### 6. **Attachments**

* None present
* **Phishing Trait:** Not applicable in this sample, but important to check