Task 2 – Phishing Email Analysis Report

Name: Pratiksha Baviskar

Task: Analyze a Phishing Email Sample

Objective: Identify phishing characteristics in a suspicious email sample.

Tools Used: Email client / saved email file (text), free online header analyser (e.g. MXToolbox Email Header Analyzer)

---

1. Sample Phishing Email

From: support@micros0ft.com
Subject: Urgent - Account Verification Required

Dear User,

We have detected unusual activity on your Microsoft account. Please verify your account immediately to avoid suspension.

Click here to verify your account: http://fake-microsoft-support-login.com

Thank you,
Microsoft Support Team

---

2. Phishing Indicators Identified

No.	Indicator	Description
✓ 1	**Suspicious Sender Address**	The sender email is **support@micros0ft.com**, with **'0' (zero) instead of 'o'**, indicating **domain spoofing**.
✓ 2	**Generic Greeting**	Uses **"Dear User"** instead of recipient's real name, indicating a mass phishing attempt.

No.	Indicator	Description
✅ 3	**Urgent Language & Threats**	Uses words like **“Urgent,” “immediately,” and “avoid suspension”** to create panic and force quick action.
✅ 4	**Suspicious URL**	The link **http://fake-microsoft-support-login.com** is **not an official Microsoft domain**.
✅ 5	**Poor Grammar / Spelling Errors**	Minor formatting issues and unprofessional sentence structure for Microsoft standards.
✅ 6	**Request for Personal Information**	Asks to **verify account by logging in via external link**, which is typical of credential harvesting.
✅ 7	**Unsecured Link (No HTTPS)**	Uses **http:// instead of https://**, indicating the page is not secured.

---

3. Header Analysis (Optional)

✅ **Tool Used:** MXToolbox Email Header Analyzer

✅ **Findings:**

- **SPF/DKIM/DMARC failed**, indicating sender spoofing.
- **Sender IP** does not match official Microsoft mail servers.

(Attach screenshot of the header analyzer output here if required by your instructor.)

---

4. Conclusion

✔ This email is confirmed as a **phishing attempt** with the goal to **steal user credentials**. It uses:

- **Domain spoofing**
- **Urgent threats**

- **Fake login pages**
  to trick users into entering their account information.