Phishing Email Analysis Report

Objective

Identify phishing characteristics in a suspicious email sample.

Tools Used

- Email (Sample Text)
- Free Header Analyzer (e.g., MXToolbox or Message Header Analyzer)

Sample Phishing Email

From: security-update@micr0soft-support.com

To: user@example.com

Subject: Urgent Action Required - Unusual Sign-in Attempt

Date: August 5, 2025

Dear user,

We detected an unusual sign-in attempt to your Microsoft account from an unknown device located in Russia. If this wasn't you, your account may be at risk. Please verify your identity immediately by clicking the secure link below:

[Verify Now](http://micros0ft-verification-login.com/secure)

Failure to act within 24 hours will result in a temporary lock on your account.

Thank you,

Microsoft Support Team

Phishing Indicators Identified

1. Suspicious Sender Address: The email is from micr0soft-support.com, not microsoft.com.
2. Urgency and Threats: Creates fear by saying your account will be locked.

Phishing Email Analysis Report

3. Unusual Location: Claims of login from Russia to scare user.

4. Malicious Link: Fake domain used in the link.

5. Generic Greeting: Uses 'Dear user' instead of real name.

6. Grammatical Errors: Minor sentence structure issues.

7. Spoofed Branding: Appears to be Microsoft but is not.

8. No Digital Signature: Lacks authentication headers.

Conclusion

The email shows clear signs of phishing. It should not be trusted and must be reported or deleted.