Phishing Email Analysis Report

Objective:

Analyze a suspicious email to identify phishing indicators using manual inspection and an online header analyzer.

Sample Email Overview:

From: support@micr0s0ft-updates.com
To: user@example.com
Subject: Urgent: Your Microsoft Account Has Been Suspended
Date: Mon, 17 Jun 2025 09:35:12 -0500

Dear Customer,

Your Microsoft account has been temporarily suspended due to suspicious login activity. To restore access, please verify your account by clicking the link below:

https://micr0s0ft-updates.com/verify

Failure to act within 24 hours will result in permanent suspension.

Sincerely,
Microsoft Support Team

[Attachment: Account_Verification_Form.docm]

Phishing Indicators Found:

1. Spoofed Email Address: support@micr0s0ft-updates.com uses zero instead of letter 'o'.
2. Suspicious Link: https://micr0s0ft-updates.com/verify has a suspicious domain.
3. Urgent Language: Threatens account suspension in 24 hours.
4. Malicious Attachment: .docm file can execute macros.
5. Email Header Issues: SPF and DKIM failed (analyzed via MxToolbox).
6. Spelling Errors: 'micr0s0ft' is a domain trick.
7. Generic Greeting: 'Dear Customer' instead of real name.
8. False Sense of Legitimacy: Attempts to mimic Microsoft branding.

Summary of Traits:

This email shows typical phishing characteristics: spoofed sender, suspicious links, urgent messaging, and malicious attachment. It's a clear attempt to steal credentials or infect the system.