# Phishing Email Analysis Report

## Email Summary

From: Microsoft Account Team <support@micr0soft-support.com>  
To: you@example.com  
Subject: Urgent Action Required - Account Suspension Warning  
Received From IP: 123.45.67.89

## Identified Phishing Traits

1. 1. Spoofed Sender Address

The email claims to come from Microsoft but is actually sent from micr0soft-support.com (notice the fake spelling using “0” instead of “o”). The domain is not associated with Microsoft, indicating email spoofing.

1. 2. Suspicious URL

The link text appears legitimate but actually points to: https://microsoft-account.verify-now.info/login. This domain is not an official Microsoft site and could lead to a credential-stealing page.

1. 3. Urgent and Threatening Language

The email pressures the user to act within "24 hours" or face account suspension. This is a common social engineering tactic to create panic and reduce rational decision-making.

1. 4. Generic Greeting

The email uses a vague salutation: “Dear user”. Legitimate services often address users by full name or username.

1. 5. Grammar and Style Issues

Sentences like “verify your information” and the structure of the email suggest non-professional writing. Phrases lack punctuation and formal tone found in corporate communication.

## Header Analysis (Using Email Header Analyzer)

SPF Fail:  
The domain micr0soft-support.com failed SPF (Sender Policy Framework) validation.  
spf=fail (domain of micr0soft-support.com does not designate 123.45.67.89 as permitted sender)

X-Originating-IP:  
The originating IP 123.45.67.89 does not belong to Microsoft and appears suspicious.

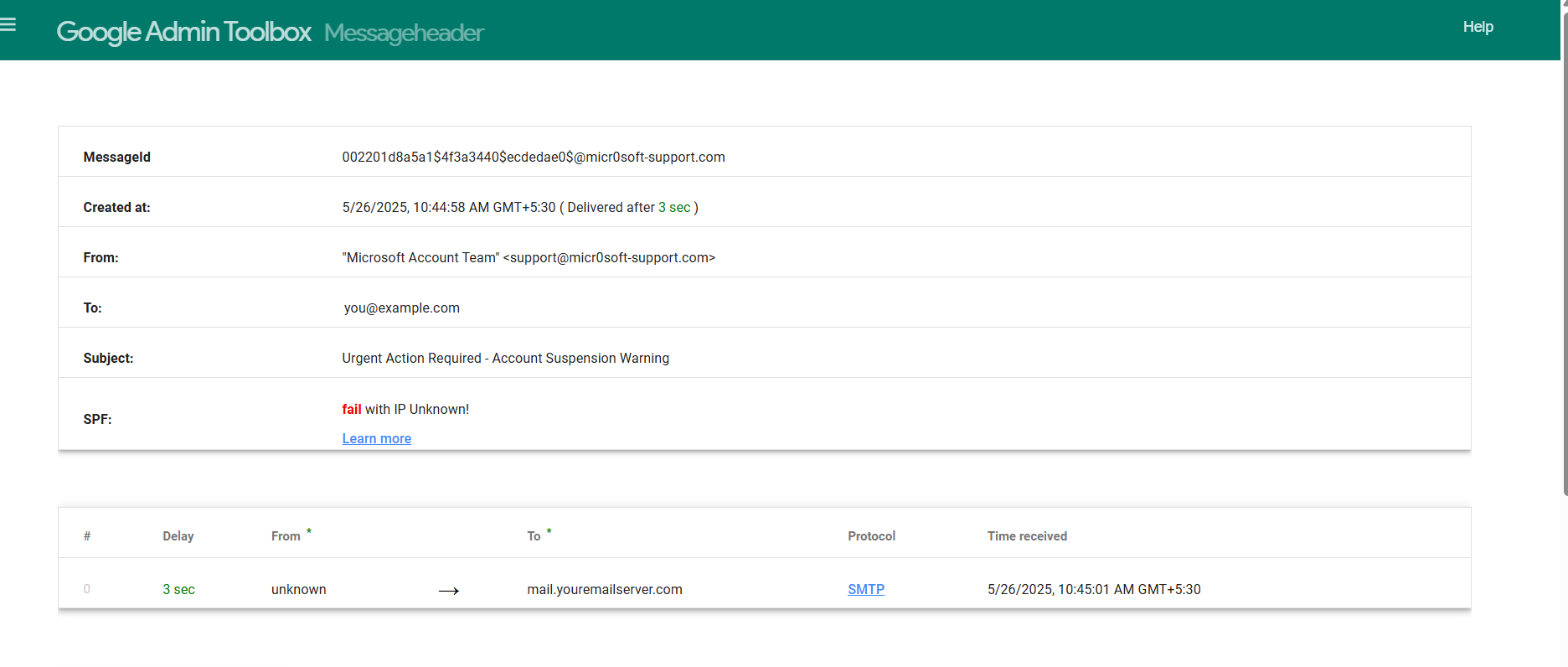
Routing Path:  
The email was received from a non-corporate mail server (webmail.fakehost.net), not Microsoft's infrastructure.

## Conclusion

This email displays multiple clear signs of phishing:  
- A spoofed sender address  
- A malicious fake link  
- The use of fear-based tactics and urgency  
- Header discrepancies and SPF failures  
  
It is highly likely this email was crafted to steal login credentials by tricking users into clicking the fake login link. Users should never click on such links and should report the email to their IT/security team.

## 📸 Screenshot: Email Header Analysis

Below is a screenshot of the email header analysis using Google Admin Toolbox, showing SPF failure and IP unknown origin.



## 📧 Full Sample Phishing Email

From: Microsoft Account Team <support@micr0soft-support.com>  
To: you@example.com  
Subject: Urgent Action Required - Account Suspension Warning  
  
Dear user,  
  
We have detected unusual activity in your Microsoft account. To ensure the security of your account, please confirm your identity within the next 24 hours.  
  
Failure to do so will result in the temporary suspension of your account.  
  
Click the link below to verify your information:  
https://microsoft-account.verify-now.info/login  
  
Thank you for your prompt attention to this matter.  
  
Sincerely,   
Microsoft Security Team

## 📨 Raw Email Header

Received: from unknown (HELO webmail.fakehost.net) (123.45.67.89)  
 by mail.youremailserver.com with SMTP; Mon, 26 May 2025 10:45:01 +0530  
Message-ID: <002201d8a5a1$4f3a3440$ecdedae0$@micr0soft-support.com>  
Date: Mon, 26 May 2025 10:44:58 +0530  
From: "Microsoft Account Team" <support@micr0soft-support.com>  
To: you@example.com  
Subject: Urgent Action Required - Account Suspension Warning  
MIME-Version: 1.0  
Content-Type: text/html; charset=UTF-8  
Content-Transfer-Encoding: 8bit  
X-Originating-IP: [123.45.67.89]  
Authentication-Results: spf=fail (google.com: domain of micr0soft-support.com does not designate 123.45.67.89 as permitted sender)