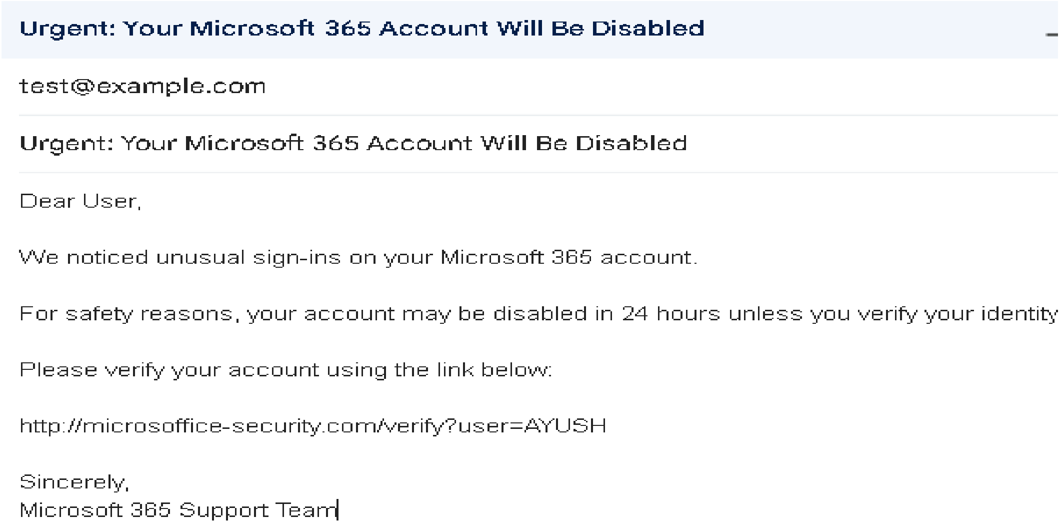
Phishing Email Examination Report

Prepared by: Ayush S.
Date: November 2025

This report examines a suspicious email designed to look like a Microsoft 365 security alert. The objective was to identify common phishing indicators using basic techniques such as checking the sender details, message content, and header analysis. A screenshot of the phishing message used for this assessment is included below.

Screenshot of the Email



Urgent: Your Microsoft 365 Account Will Be Disabled

test@example.com

Urgent: Your Microsoft 365 Account Will Be Disabled

Dear User,

We noticed unusual sign-ins on your Microsoft 365 account.

For safety reasons, your account may be disabled in 24 hours unless you verify your identity

Please verify your account using the link below:

http://microsoffice-security.com/verify?user=AYUSH

Sincerely,
Microsoft 365 Support Team

Email Summary
Sender Name: Support
Sender Email: support@microsoffice-security.com
Subject: Urgent: Your Microsoft 365 Account Will Be Disabled
Type of Email: Suspicious / Phishing
Reason for Checking: The email requested urgent account verification, which looked unusual.

Raw Email Headers (Sample)
Return-Path: <support@microsoffice-security.com>
Received-SPF: Fail
Authentication-Results: dkim=none; spf=fail; dmarc=none
Received: from unknown server – originating IP did not match Microsoft servers.

Findings (Explained in Simple Language)

1. The sender address was suspicious. The domain used was not related to Microsoft.
2. SPF check failed, indicating the sender server was not authorized.
3. The verification link did not lead to an official Microsoft domain.
4. The email used urgency to pressure the user into clicking the link.
5. The formatting lacked professional structure and did not include official branding.

Conclusion
Based on the analysis, the email is a phishing attempt. It uses a fake domain, fails authentication

checks, and includes a suspicious link. The email should not be trusted or interacted with.

Recommendations

- Do not click on suspicious links.
- Always verify the sender address properly.
- Use email header analysis tools when unsure.
- Report phishing emails through the mail provider’s reporting function.