# Phishing Email Analysis Report

Date: May 27, 2025

Analyst: Saikumar

Subject: Your Account Will Be Suspended – Action Required

## 1. Sample Phishing Email

From: "Microsoft Support" <support-secure@m1crosoft-account.com>  
To: user@example.com  
Subject: Your Account Will Be Suspended – Action Required  
Date: May 27, 2025  
  
Dear User,  
  
We detected suspicious activity on your Microsoft account. For your safety, we have temporarily suspended access.  
  
Please verify your identity by clicking the secure link below:  
  
👉 https://microsoft-account-verification.com/login  
  
Failure to act within 24 hours will result in permanent account suspension.  
  
Thank you,   
Microsoft Security Team  
  
Attachment: Security\_Document.pdf.exe

## 2. Phishing Indicators and Analysis

### 2.1 Sender Address Analysis

The sender's address (support-secure@m1crosoft-account.com) is a spoofed domain. It uses a lookalike domain with the number '1' instead of the letter 'i' to mimic a legitimate Microsoft domain. This is a common phishing tactic.

### 2.2 Email Header Check

If analyzed through a header analyzer, discrepancies may be found such as mismatched Return-Path (e.g., no-reply@randommail.ru), failed SPF, DKIM, or DMARC records, indicating potential spoofing.

### 2.3 Suspicious Links and Attachments

The email includes a suspicious link (https://microsoft-account-verification.com/login), which is not a legitimate Microsoft domain. It is likely a phishing page designed to steal credentials. The attachment 'Security\_Document.pdf.exe' has a double file extension, indicating it's a disguised executable and likely malicious.

### 2.4 Urgent or Threatening Language

The email uses scare tactics such as threatening permanent account suspension within 24 hours to pressure the user into acting quickly.

### 2.5 Mismatched URLs

Hovering over the displayed link would reveal it leads to a different, malicious domain. This mismatch is a clear phishing indicator.

### 2.6 Spelling and Grammar Errors

Although there are no obvious spelling errors, the tone is generic and impersonal. Legitimate communications from Microsoft usually address the user by name and contain official branding.

## 3. Summary of Phishing Traits

|  |  |
| --- | --- |
| Indicator | Details |
| Spoofed Sender | m1crosoft-account.com mimics Microsoft |
| Suspicious Link | Fake Microsoft verification domain |
| Malicious Attachment | .exe file disguised as a PDF |
| Urgency | Threatens account suspension in 24 hours |
| Mismatched URL | Displayed link differs from actual link |
| Generic Content | No personalized greeting or branding |