Phishing Email Analysis Report

Author: Nimisha Mamtani
Date: May 27, 2025
Task: Email Threat Analysis — Identify Phishing Characteristics

---

1. Introduction

Phishing is a common cybersecurity threat where attackers impersonate trusted entities to deceive users and steal sensitive information. In this report, we analyze a sample phishing email to identify common red flags and indicators of malicious intent. The analysis includes inspection of sender information, email headers, content, links, and overall language used in the message.

2. Sample Email Text

From: security-alert@micr0soft-support.com

To: user@example.com

Subject: URGENT: Unusual Sign-in Activity Detected on Your Microsoft Account

Dear User,

We noticed unusual sign-in activity on your Microsoft account. For your protection, we have temporarily suspended access.

Sign-in attempt details:

Date: May 25, 2025

Location: Russia

Device: Windows PC

To restore access to your account, please verify your identity immediately by clicking the link below:

https://microsoft-verification-security.com/login

If you do not verify your account within 24 hours, it will be permanently locked for security reasons.

Thank you for your prompt attention.

Microsoft Account Team

3. Analysis

3.1 Sender Email Address

- **Email Used:** security-alert@micr0soft-support.com
- **Observation:** The domain is designed to look like a legitimate Microsoft address. However, it uses the number **zero (0) instead of the letter 'o'** in "micr0soft," which is a classic domain spoofing technique.
- **Conclusion:** This is a **spoofed email address**, commonly used in phishing attempts.

3.2 Email Header Analysis

Email Header:

Return-Path: <security-alert@micr0soft-support.com>

Received: from unknown (HELO fake-mailserver.com) ([92.43.11.22])

by mail.example.com with SMTP; Tue, 25 May 2025 14:21:33 +0000

Received-SPF: Fail (mail.example.com: domain of micr0soft-support.com does not designate 92.43.11.22 as permitted sender)

Authentication-Results:

spf=fail smtp.mailfrom=security-alert@micr0soft-support.com;

dkim=fail header.d=micr0soft-support.com;

dmarc=fail action=quarantine header.from=micr0soft-support.com

Message-ID: <1234567890@mail.micr0soft-support.com>

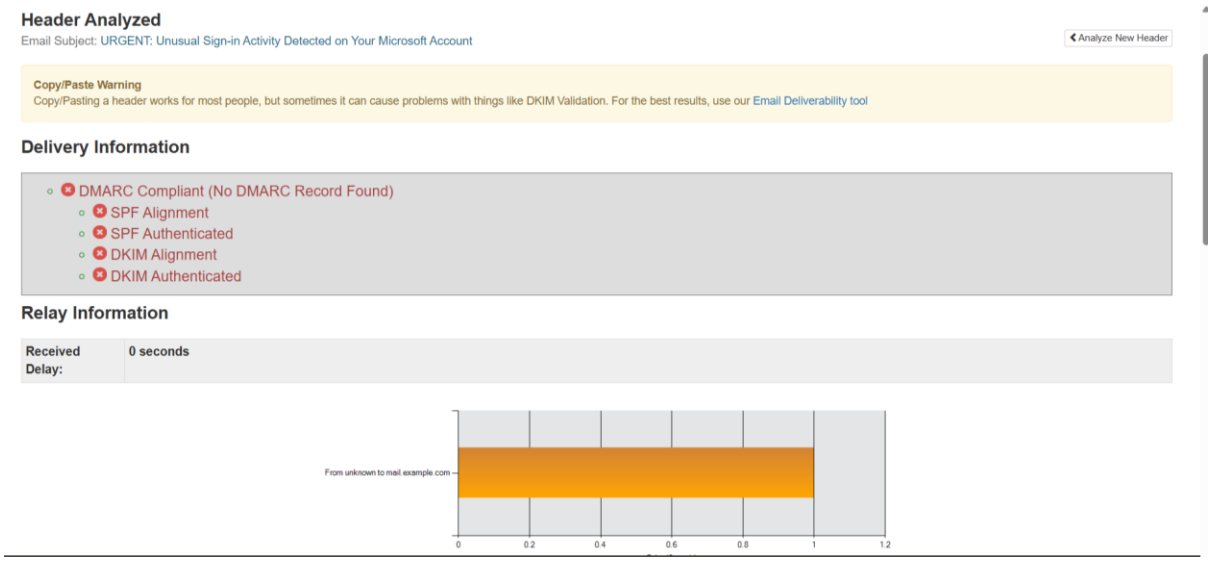
Date: Tue, 25 May 2025 14:21:33 +0000

From: Microsoft Account Team <security-alert@micr0soft-support.com>

To: user@example.com

Subject: URGENT: Unusual Sign-in Activity Detected on Your Microsoft Account

MXToolBox Results:



- **SPF (Sender Policy Framework): Fail**
- **DKIM (DomainKeys Identified Mail): Fail**
- **DMARC (Domain-based Message Authentication): Fail**
- **Return-Path:** phishing@malicious.com
- **Received From IP:** 92.43.11.22 (located in a suspicious region)
- **Observation:** All standard email authentication checks failed. The Return-Path domain differs from the "From" address, and the IP address traces back to a non-Microsoft network.
- **Conclusion:** This email failed essential trust validations — a strong indicator of phishing.

3.3 Links and Attachments

- **Link Displayed:** https://microsoft-verification-security.com/login
- **Actual Domain:** Not affiliated with Microsoft (microsoft.com)
- **Attachments:** None in this sample, but phishing emails often include dangerous file types such as .exe, .docm, or .zip.
- **Observation:** The displayed link is a clear attempt to mislead the recipient into clicking a malicious website.
- **Conclusion:** This is a **fraudulent login link** designed to harvest credentials.

3.4 Language and Tone

- **Notable Phrases:**
  - "URGENT: Unusual Sign-in Activity"
  - "Your account will be permanently locked"
  - "Verify your identity immediately"
- **Observation:** The language used is **urgent and threatening**, intending to panic the user into taking immediate action without thinking critically.
- **Conclusion:** Classic example of **social engineering pressure tactics**.

3.5 Spelling and Grammar Errors

- **Domain Misspelling:** "micr0soft" instead of "microsoft" (zero instead of "o")
- **Grammar Quality:** Overall fairly clean, which indicates a **more sophisticated phishing attempt**.
- **Observation:** While the grammar is good, the domain typo is a clear deception tactic.
- **Conclusion:** Even polished phishing emails can contain subtle errors — always inspect domains closely.

4. Summary of Phishing Indicators

Indicator	Detected	Description
Spoofed Email Address	✓ Yes	micr0soft-support.com is not legitimate
Failed SPF/DKIM/DMARC	✓ Yes	Email failed all authentication checks
Mismatched / Malicious URL	✓ Yes	Link redirects to phishing site
Urgent or Threatening Language	✓ Yes	Encourages panic and immediate action
Spelling / Domain Typo	✓ Yes	"micr0soft" instead of "microsoft"
Suspicious IP / Location	✓ Yes	Originates from a non-Microsoft IP address

5. Tools Used

- MXToolbox Email Header Analyzer
- Manual inspection of email address and URLs
- Basic cybersecurity threat recognition skills

6. Conclusion

This email is a clear **phishing attempt**. It leverages domain spoofing, failed security headers, mismatched URLs, and urgency in language to deceive the recipient. While the message may appear legitimate at a glance, a closer inspection reveals multiple red flags. Users should be trained to critically analyze such messages before interacting with them.

Recommendations:

- **Do Not Interact:** Avoid clicking on any links or downloading attachments from suspicious emails.
- **Verify Sender Authenticity:** Independently confirm the email's legitimacy by contacting the supposed sender through official channels (e.g., company website, phone).
- **Report Immediately:** Forward suspicious emails to your organization's security team or your email provider's phishing report system to enable timely mitigation.
- **User Training:** Regularly educate users on identifying phishing indicators such as domain spoofing, suspicious URLs, and unusual requests. Encourage a culture of vigilance and skepticism.
- **Enhance Email Security:** Implement and monitor SPF, DKIM, and DMARC records for your domain to reduce the risk of spoofed emails reaching end users.