

Phishing Email Analysis Report

1. Introduction

This report aims to identify phishing characteristics in a suspicious email. By analyzing the email's content, headers, and links, this exercise enhances awareness of phishing tactics and strengthens skills for email threat analysis.

2. Sample Phishing Email

A sample phishing email was obtained from the website: Phishing Examples - [Phishing.org](https://www.phishing.org).

Screenshot 1: Sample Phishing Email

From: Apple Support <support@apple.verify-login.com>

Subject: Your Apple ID has been suspended



Dear Customer,

Your Apple ID has been suspended. Immediate action is required to restore access.

Please verify you informations by click the link bellow.

<https://apple.com/account/login>

Sincerely,

Apple Support

3. Email Header Analysis

The email header was extracted from the email client and analyzed using the online tool: MXToolbox Email Header Analyzer.

Screenshot 2: Email Header in Analyzer

Header Analysis	
Header:	Explanation
Return-Path: support@apple.verify-login.com Authentification-Results: mxtoolbox.com spf=fail reason: domain apple,verify-login.com does not designate 103.12.96.24 as permitted sender dkim=fail reason: No valid signature dmarc=none reason: No valid DMARC record Received from example,test [103.12.96.24] by mail1.fakeserver.local with SMTP From: Apple Support <support@apple.verify-login.com> Date: Mon, 15 Apr 2024 08:00:00 -0800 Subject: Your Apple ID has been suspended	 Return-Path domain does not match sender domain. FAIL Received from a different server INFO SPF Check for 103.12.96.24 fails FAIL DKIM Check FAIL DMARC Check No valid record found FAIL Three are

Findings:

- **Return-Path** domain does not match the sender's domain.
- **Received From:** Indicates redirection from an unexpected server.
- **SPF/DKIM/DMARC Failures:** The sender failed authentication checks.

4. Sender Address Spoofing

- **Displayed Email Address:** support@apple.com
- **Actual Email Address:** support@apple.verify-login.com

⚠ The actual sender domain is spoofed to appear like a legitimate Apple domain.

5. Suspicious Links

Visible Link: <https://apple.com/account/login>

Actual Link (on hover): <http://verify-apple-login.com/phish>

⚠ Mismatched URL designed to steal login credentials.

Screenshot 3: Hover-over Link Showing Fake URL

Dear Customer,

Your Apple ID has been suspended for security reasons due to an unusual activity.

[To restore your account, please click on](#)

<https://www.example.com/restore-account>


Sincerely,

Apple Support

6. Urgent or Threatening Language

Email Body Extract:

"Your Apple ID has been suspended. Immediate action is required to restore access."

 This creates a sense of urgency and panic to trick the recipient into clicking the link.

7. Attachments

- No attachment in this sample. However, phishing emails often use **.zip**, **.exe**, or fake **.pdf** files to deliver malware.
-

8. Grammar and Spelling Errors

"Please verify your information by clicking the link below."

 Poor grammar and spelling mistakes are typical signs of phishing.

9. Summary of Phishing Traits Identified

#	Indicator	Description
1	Spoofed Email Address	Sender appears to be Apple but uses a fake domain
2	Header Discrepancies	SPF/DKIM checks failed; mismatch in return-path
3	Mismatched URLs	Link text and destination URL do not match
4	Urgency Language	Tries to scare user into clicking the link
5	Spelling Errors	Unprofessional language in the email
6	Generic Greeting	"Dear Customer" instead of real name (not personalized)

10. Conclusion

This phishing email employs several common tactics such as spoofing, mismatched URLs, urgency, and poor grammar to deceive the recipient. Awareness of these indicators is critical in avoiding email-based cyber threats.

11. References

- Phishing Examples - Phishing.org
- MXToolbox Email Header Analyzer
- [Have I Been Pwned](#) (for checking exposed accounts)