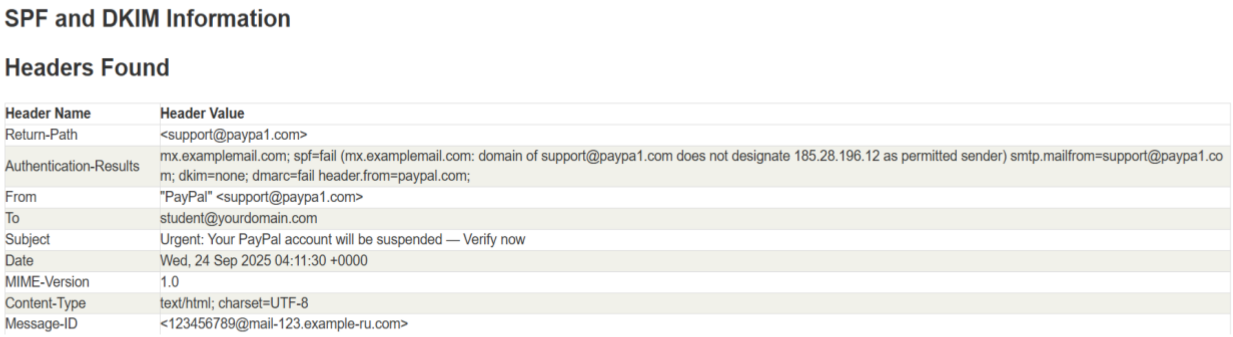
Phishing Email Analysis Report — Task 2

Analyst: Arshiya Sulthana
Date: 24 September 2025
Sample Source: phish_sample.txt (synthetic phishing sample)

1. Sender analysis

- **From:** "PayPal" <support@paypa1.com>
- **Return-Path:** <support@paypa1.com>
- **Observation:** The email uses a **look-alike domain** (paypa1.com vs paypal.com) — this is a common impersonation -> **SPOOFING** tactic.

2. Header analysis (evidence)



SPF and DKIM Information

Headers Found

Header Name	Header Value
Return-Path	<support@paypa1.com>
Authentication-Results	mx.examplemail.com; spf=fail (mx.examplemail.com: domain of support@paypa1.com does not designate 185.28.196.12 as permitted sender) smtp.mailfrom=support@paypa1.com; dkim=none; dmarc=fail header.from=paypal.com;
From	"PayPal" <support@paypa1.com>
To	student@yourdomain.com
Subject	Urgent: Your PayPal account will be suspended — Verify now
Date	Wed, 24 Sep 2025 04:11:30 +0000
MIME-Version	1.0
Content-Type	text/html; charset=UTF-8
Message-ID	<123456789@mail-123.example-ru.com>

Interpretation: Authentication checks failed (SPF) and DKIM is not present. The sending IP and server do not belong to PayPal, which strongly indicates the message is forged.

3. Links & attachments

- **URL:** http://secure-paypal.verify-account-login.ru/confirm — **mismatched domain** (not paypal.com)
- **Attachments:** None in this sample.

Risk: The link points to a suspicious domain (verify-account-login.ru) designed to mimic PayPal. Clicking it may lead to credential theft or malware.

4. Language & social-engineering indicators

- **Urgent / threatening language:** "Failure to verify within 24 hours will result in permanent suspension." — **classic pressure tactic** to force quick action.

5. Risk assessment

- **Severity: HIGH**
- **Why:** Multiple technical authentication failures (SPF/DKIM/DMARC) + impersonation (look-alike domain) + mismatched URL + urgent social engineering.

6. Conclusion

This email is **conclusively a phishing attempt**. The combination of **authentication failures**, a **spoofed sender**, **mismatched URLs**, and **urgent social engineering** shows it was crafted to trick recipients into surrendering credentials.

Prepared by: Arshiya Sulthana
Notes: I saved the header analyzer output and recommend attaching a screenshot of the analyzer results.