**Task 2: Analyze a Phishing Email Sample.**

**✉️ Email Overview**

* Subject: Urgent: Your Account Will Be Suspended in 24 Hours
* From: Security Team <support@secure-paypal-verify.com>
* To: victim@example.com
* Date: 4 August 2025

**phishing\_email.txt**  
Subject: Urgent: Your Account Will Be Suspended in 24 Hours

From: Security Team <support@secure-paypal-verify.com>

Date: Mon, 4 Aug 2025 09:34:56 -0400

To: victim@example.com

Dear Customer,

We noticed unusual activity on your PayPal account.

Please verify your identity immediately to avoid suspension.

Click the link below to verify:

http://paypal-security-verify-login.com

phishing\_email.txt

Thank you,

PayPal Security Team.  
  
  
**email\_headers.txt**

Return-Path: <support@secure-paypal-verify.com>

Received: from unknown (HELO server1.example.com) (203.0.113.55)

by mail.example.com with ESMTP; Mon, 4 Aug 2025 09:34:56 -0400

Received-SPF: fail (example.com: domain of support@secure-paypal-verify.com does not designate 203.0.113.55 as permitted sender)

Authentication-Results: mail.example.com; spf=fail smtp.mailfrom=support@secure-paypal-verify.com; dkim=fail header.d=paypal.com

Message-ID: <1234567890@example.com>

Date: Mon, 4 Aug 2025 09:34:56 -0400

From: Security Team <support@secure-paypal-verify.com>

To: victim@example.com

Subject: Urgent: Your Account Will Be Suspended in 24 Hours

**analyze\_headers.py**  
import re

def analyze\_headers(header\_file):

with open(header\_file, 'r') as f:

headers = f.read()

issues = []

if "spf=fail" in headers.lower():

issues.append("SPF authentication failed.")

if "dkim=fail" in headers.lower():

issues.append("DKIM authentication failed.")

from\_match = re.search(r"From: .\*<(.+?)>", headers)

if from\_match:

sender\_email = from\_match.group(1)

if not sender\_email.endswith("@paypal.com"):

issues.append(f"Suspicious sender domain: {sender\_email}")

return issues

if \_\_name\_\_ == "\_\_main\_\_":

problems = analyze\_headers("email\_headers.txt")  
print("Header Analysis Issues Found:")

for p in problems:

print(f"- {p}")  
  
**1. Sender Email Check**

* The sender domain `secure-paypal-verify.com` is not an official PayPal domain (`paypal.com`).
* Likely spoofed to impersonate PayPal.

**2. Email Header Findings**

Tool Used: Google Admin Toolbox Messageheader

* SPF: Failed – sending IP is not authorized.
* DKIM: Failed – signature mismatch.
* Sending server IP is unrelated to PayPal’s infrastructure.

**3. Suspicious Links**

* Displayed Link: "Verify Now"
* Actual Link (hover result): `http://paypal-security-verify-login.com`
* The domain is unrelated to PayPal.

**4. Urgent/Threatening Language**

* “Your account will be suspended in 24 hours”
* Creates panic to make the recipient act quickly.

**5. Grammar/Formatting Issues**

* Slight grammatical mistakes and awkward phrasing.

**Summary of Phishing Indicators**

* + Fake sender domain.
  + Failed SPF/DKIM authentication.
  + Suspicious non-PayPal link.
  + Urgent threat to account access.
  + Minor grammar issues.

**Conclusion:**

The email is a phishing attempt aiming to steal PayPal credentials.

Action taken: Marked as phishing and reported to PayPal’s security team.

