**TASK- 2**

**Phishing Email Analysis Report**

**Email Overview**

* **Subject: Urgent**: Suspicious Activity Detected on Your PayPal Account
* **Sender Name:** PayPal Security
* **Sender Email Address:** security-alert@paypal-support.com
* **Recipient:** youremail@example.com
* **Link Displayed:** verify your account (anchor text)
* **Actual Link:** https://paypal-security-check.com/verify

**Phishing Indicators Identified**

**1. Suspicious Sender Email Address**

* The sender uses paypal-support.com which is not an official PayPal domain.
* Legitimate PayPal emails come from @paypal.com.

**2. Spoofed Display Name**

* The name "PayPal Security" is used to impersonate a trusted entity.
* Attackers often use official-sounding names to gain user trust.

**3. Urgent and Fear-Inducing Language**

* Phrases like “Suspicious Activity Detected” and “Failure to verify within 24 hours will result in permanent suspension” are used to create panic.
* This is a common social engineering tactic.

**4. Deceptive Link with Anchor Text**

* The visible link text says “verify your account”, but it actually leads to a malicious domain:  
  https://paypal-security-check.com/verify
* Legitimate companies rarely ask users to click such links via email.

**5. Generic Greeting**

* Uses “Dear Customer” instead of addressing the recipient by name.
* Most official services personalize their emails.

**6. No Contact Information**

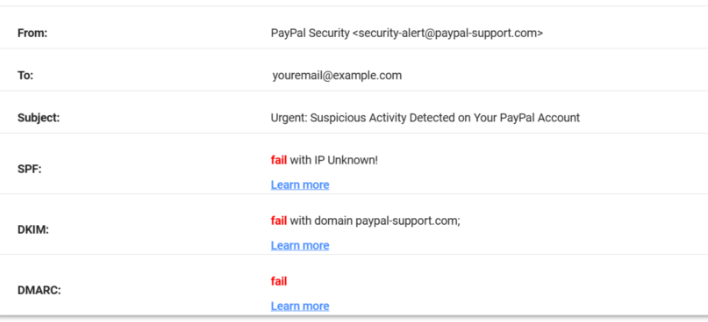
* There's no official PayPal address, phone number, or customer support link.
* Lack of legitimate contact details is suspicious.

**7. Spelling & Grammar**

* While the sample has no errors, attackers often include:
  + “We have detect unusual activity…” (should be “detected”)
  + “acount” instead of “account” (not in this one, but watch for this)

**Email Header Analysis**

Tool used - toolbox.googleapps.com



**Email Sample Txt**

From: PayPal Security [security-alert@paypal-support.com](mailto:security-alert@paypal-support.com)

To: [youremail@example.com](mailto:youremail@example.com)

Subject: Urgent: Suspicious Activity Detected on Your PayPal Account

Dear Customer,

We have detected unusual activity on your PayPal account. For your protection, we have temporarily limited your account access.

Please [verify your account](https://paypal-security-check.com/verify) to restore full access and avoid service interruption.

Failure to verify within 24 hours will result in permanent suspension of your account.

Thank you,

PayPal Support Team

Note: This is an automated message. Please do not reply to this email.

**Fake Email Header. Txt**

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

Received: from unknown (HELO mail.paypal-support.com) (123.45.67.89)

by mail.example.com with SMTP; Tue, 05 Aug 2025 11:16:45 +0000

Received-SPF: Fail (example.com: domain of paypal-support.com does not designate 123.45.67.89 as permitted sender)

Authentication-Results: example.com;

dkim=fail header.i=@paypal-support.com;

spf=fail smtp.mailfrom=paypal-support.com;

dmarc=fail (p=REJECT) header.from=paypal-support.com

Message-ID: <001a113000b5117a@paypal-support.com>

Date: Tue, 05 Aug 2025 11:16:45 +0000

From: PayPal Security <security-alert@paypal-support.com>

To: youremail@example.com

Subject: Urgent: Suspicious Activity Detected on Your PayPal Account

MIME-Version: 1.0

Content-Type: text/html; charset=UTF-8