**Task- 2**

1. **Sample Phishing Email**

From: PayPal <support@paypai.com>

Subject: Urgent: Account Suspended – Immediate Action Required

Dear Customer,

We noticed suspicious activity in your account. Your access has been temporarily limited. To restore full access, please verify your information by clicking the link below:

[Click here to verify your account](http://paypai-security-alert.com/verify)

Failure to respond within 24 hours will result in permanent suspension.

Sincerely,

PayPal Security Team

1. **Sender's Email Address (Spoof Check)**

**Claimed Address:** support@paypai.com

**Legit Domain:** paypal.com

1. **Email Header Analysis**

**Possible Findings:**

* SPF/DKIM failed or missing
* Return-path doesn’t match sender domain
* IP address not associated with PayPal

1. **Suspicious Links or Attachments**

 Link text: Click here to verify your account

 Actual link (on hover): <http://paypai-security-alert.com/verify>

1. **Urgent or Threatening Language:**

 “Immediate Action Required”

 “Failure to respond… will result in permanent suspension”

1. **Mismatched URLs:**

 Visible vs actual link mismatch.

 Hovering reveals non-PayPal domain.

1. **Spelling or Grammar Errors:**

 “Paypai” (intentional typo)

 Unnatural phrases like “restore full access”

1. **Summary of Phishing Traits:**

| **Trait** |  | **Details** |
| --- | --- | --- |
| Spoofed Email |  | paypai.com instead of paypal.com |
| Urgent Language |  | Threat of account suspension |
| Suspicious Links |  | Mismatched and malicious URL |
| Header Anomalies |  | Likely forged headers (SPF/DKIM issues) |
| Grammar Errors |  | Minor unnatural phrasing |
| Attachment or Link |  | Dangerous link to fake login page |