**TASK 3**

### **Email Analysis**

#### **Email**:

From: support@paypa1.com

To: victim@example.com

Subject: Your Account Has Been Limited – Action Required

Dear Valued Customer,

Your PayPal account has been temporarily suspended due to suspicious activity. To restore your account, please verify your identity by clicking the link below:

[Verify Your Account](http://secure-paypal-login.com)

If you do not complete this process within 48 hours, your account will be permanently disabled.

Thank you,

PayPal Security Team

### **Analysis**

#### **1. Header Analysis**

* **Sender Address**:
  + support@paypa1.com looks similar to paypal.com, but the domain is fake.
* **Return Path**:
  + Often different from the sender address in phishing emails.
* **Received From**:
  + IP address or server details may indicate an unusual location (e.g., not from PayPal's servers).

#### **2. Body Analysis**

* **Content**:
  + Urgency: "Your account has been temporarily suspended" creates fear.
  + Grammar: Minor issues in phrasing, such as "If you do not complete this process..."
* **Link Analysis**:
  + Hovering over [Verify Your Account] reveals http://secure-paypal-login.com, which is not a legitimate PayPal domain.

#### **3. Attachment Analysis**

* No attachments in this example, but phishing emails may include:
  + Malicious documents (.docx, .pdf) with embedded malware.
  + Executable files (.exe).

#### **4. Tools for Verification**

* **Email Header Tools**:
  + Use tools like [MXToolbox](https://mxtoolbox.com/) to analyze email headers and verify sender IP addresses.
* **URL Verification**:
  + Use [VirusTotal](https://www.virustotal.com/) to scan suspicious URLs.
* **Attachment Scanning**:
  + Use a sandbox like [Hybrid Analysis](https://www.hybrid-analysis.com/) for malware detection.

### **Red Flags Identified**

1. **Sender Address Spoofing**:
   * support@paypa1.com is designed to look like paypal.com.
2. **Fake Domain**:
   * http://secure-paypal-login.com is not associated with PayPal.
3. **Urgency and Fear**:
   * Threats of account suspension push the user to act without thinking.
4. **Generic Greeting**:
   * Legitimate companies often address users by name, not "Dear Valued Customer."
5. **Unusual Links**:
   * Hovering over the link shows a domain unrelated to PayPal.

### **Recommendations to Avoid Such Attacks**

1. **Verify the Sender**:
   * Check the sender’s email address carefully for typos or mismatched domains.
2. **Hover Over Links**:
   * Verify URLs before clicking; legitimate websites use HTTPS and correct domains.
3. **Avoid Attachments**:
   * Do not open unexpected attachments, especially from unknown senders.
4. **Two-Factor Authentication (2FA)**:
   * Enable 2FA to secure your accounts.
5. **Educate Users**:
   * Regular training on phishing awareness for employees and individuals.

### **Report: Email Analysis**

#### **Title**: Phishing Email Analysis Report

#### **1. Overview**

* **Objective**: Analyze a phishing email claiming to be from PayPal.
* **Key Findings**: The email is fraudulent and uses multiple phishing tactics to deceive the user.

#### **2. Red Flags Identified**

| **Indicator** | **Details** |
| --- | --- |
| **Sender Address** | support@paypa1.com (spoofed to resemble paypal.com). |
| **Fake Domain in Link** | http://secure-paypal-login.com (not PayPal's legitimate domain). |
| **Urgent Language** | "Your account has been temporarily suspended" creates fear and urgency. |
| **Generic Greeting** | "Dear Valued Customer" instead of addressing the recipient by name. |
| **Suspicious Links** | Link domain mismatched with PayPal's official domain (paypal.com). |

#### **3. Tools Used**

1. **Header Analysis**: Manual inspection and MXToolbox.
2. **URL Scanning**: VirusTotal.
3. **Sandbox for Attachments**: N/A (no attachments in this email).

#### **4. Recommendations**

1. **Verify sender details** and domain authenticity.
2. **Enable email filtering** to block suspicious emails.
3. **Educate users** on identifying phishing tactics.
4. **Enable 2FA** for all sensitive accounts.