Task 5: Email Analysis Report

1. Email Sample (Phishing Attempt)

**Subject:** Urgent: Your Account Will Be Suspended!  
**From:** [support@secure-paypal.com](mailto:support@secure-paypal.com)  
**To:** [yourname@example.com](mailto:yourname@example.com)

*Dear Customer,  
We have detected unusual activity in your PayPal account. For your protection, your account will be suspended within 24 hours unless you verify your information.*

*Please click the link below to verify your account and prevent suspension:*[*https://paypal-secure-login.com/verify*](https://paypal-secure-login.com/verify)

*If you do not complete this verification, your account access will be permanently restricted.*

*Thank you for your prompt attention to this matter.*

*Best regards,  
PayPal Security Team*

***Attachment:****PayPal\_Verification\_Form.zip*

2. Red Flags Identified

* **Suspicious Sender Address:**  
  The email is sent from support@secure-paypal.com instead of an official PayPal domain (e.g., @paypal.com).
* **Urgent and Threatening Language:**  
  The message threatens account suspension to create panic and force quick action.
* **Suspicious Link:**  
  The link provided (paypal-secure-login.com) is not PayPal’s official website and could lead to a phishing page.
* **Generic Greeting:**  
  The email addresses the recipient as "Dear Customer" instead of using their real name.
* **Unexpected Attachment:**  
  The email contains a .zip file attachment, which is commonly used to deliver malware.
* **Request for Sensitive Information:**  
  The email asks the recipient to verify their account, which is a common tactic for stealing login credentials.
* **Poor Grammar or Formatting:**  
  (If present) Look for spelling mistakes or awkward phrasing, which are common in phishing emails.

3. Risks Involved

* **Credential Theft:**  
  Clicking the link may lead to a fake website designed to steal PayPal login details.
* **Malware Infection:**  
  Downloading or opening the attached .zip file could install malware or ransomware on the recipient’s device.
* **Financial Loss:**  
  If credentials are stolen, attackers could access the victim’s PayPal account and perform unauthorized transactions.

4. Recommendations to Avoid Such Attacks

* **Verify Sender’s Email Address:**  
  Always check if the sender’s domain matches the official company domain.
* **Do Not Click Suspicious Links:**  
  Hover over links to preview the URL. Only click if you are sure it is legitimate.
* **Avoid Opening Unexpected Attachments:**  
  Do not open attachments from unknown or untrusted sources.
* **Look for Personalized Greetings:**  
  Legitimate companies usually address you by your real name.
* **Enable Two-Factor Authentication:**  
  Add an extra layer of security to your accounts.
* **Educate Yourself and Others:**  
  Stay informed about common phishing tactics and share knowledge with friends and colleagues.
* **Contact the Company Directly:**  
  If you receive a suspicious email, contact the company using official channels (not the contact details in the email).

**Prepared by:** Kamala Majila  
**Date:** 20 June 2025