Task 2: Phishing Email Analysis Report

- **Name**: Rishika Gupta
- **Date**: 05.08.25

The purpose of this task is to analyze a sample phishing email and identify common traits used by attackers, such as spoofed sender addresses, suspicious links, and psychological manipulation.

1st sample from PhisTank

From: support@paypa1.com Subject: Urgent Action Required – Account Suspended!

Dear Customer,

We have noticed suspicious activity on your PayPal account. To avoid permanent suspension, please verify your account immediately by clicking the link below:

Click here to verify

Failure to respond within 24 hours will result in account termination.

Thank you, PayPal Security Team

Analysis:

a. Sender's Email Address

- Spoofed: `support@paypa1.com` (uses "1" instead of "l" in "paypal")
- Tries to imitate an official PayPal email

b. Suspicious Links or Attachments

- Link appears to be: `http://paypal-verification-alert.com`
- Hover shows mismatch from actual PayPal URL
- No attachments, but link is malicious

c. Urgent or Threatening Language

- Phrases like “Urgent Action Required” and “account will be suspended” create panic

d. Mismatched URLs

- Link text may say one thing, actual destination is different
- Used to trick users into clicking

e. Spelling/Grammar Errors

- Slight awkwardness: “Failure to respond… will result in account termination.”
- Generic greeting: “Dear Customer” instead of your name

2. Email Summary

- **Subject**: Congratulations! You’ve Been Selected for multiple interviews - Schedule Your Interview Now
- **From**: Sushmita Sharma | HR Team <`sanjoli.raj@freshersindia.in`>
- **To**: RISHIKA KUMARI
- **Date**: Thu 31/07/2025 6:48 PM
- **Call to Action**: [To Apply Click Here]
- **Message Body Highlights**:
    - Mention of ₹15.7 LPA salary
    - Urgency to complete your profile to avoid cancellation
    - Encouraging tone, promising “top MNC interviews”

Phishing Analysis

1. Sender's Email Address

- `sanjoli.raj@freshersindia.in` looks **semi-professional**, but:
    - It uses an **unknown domain**, not a known company like `tcs.com`, `infosys.com`, or `freshersworld.com`
    - The mismatch between **name and email ID** (Sushmita Sharma vs. Sanjoli Raj) is suspicious

🚩 **Red Flag**: Sender name doesn't match email address.

2. Email Header (Not fully visible, so assumptions made)

If analyzed, it may show:

- **SPF/DKIM/DMARC failures**
- Possibly sent via a **bulk mailing server** (not from a real HR department)

3. Suspicious Link

- Text: **"[To Apply Click Here]"**
- **Link destination is hidden** in the screenshot — a common phishing trick
    - Likely redirects to a fake job portal or credential harvesting page

🚩 **Red Flag**: Clickable link with unclear destination — always dangerous.

4. Urgency or Pressure Tactics

- Uses phrases like:
    - “Schedule your interview at the earliest”
    - “Incomplete profiles may lead to cancellation”

🚩 **Red Flag**: Creates a false sense of urgency — a hallmark of phishing.

5. Spelling / Grammar

- Grammar is mostly fine
- But phrases like:
    - “top most leading names in the industry” (awkward wording)
    - “advance your career with Top MNC” (capitalization odd)

⚠️ **Minor Warning**: Unnatural sentence structure

6. Too Good to Be True

- “Salary Package: ₹15.7 LPA” with **no company name or role mentioned**
- Massively high offer for an unspecified job

🚩 **Red Flag**: Unrealistic offer + lack of job details = likely bait