Elevate Labs (Task 2)

1) Obtain a sample phishing email

From: support@paypa1.com

Subject: Urgent: Your Account Has Been Suspended

Dear Customer,

We noticed unusual activity in your PayPal account and have temporarily limited your access for security reasons.

To restore your account access, please verify your information immediately by clicking the secure link below:

[Verify Your Account Now](http://paypal-verification-security.com/login)

Failure to comply within 24 hours will result in permanent account suspension.

Thank you for choosing PayPal.

Sincerely,

PayPal Security Team

2) Examine Sender’s email address for spoofing

- support@paypa1.com looks similar to PayPal but uses paypa1 (with a number 1 instead of "l")

3) Check email header for discrepancies

- SPF/DKIM failures
- Unusual Return-Path or Reply-To domains
- Mismatch between From and sending server Ips

4) Identify suspicious link or attachments

- Link: http://paypal-verification-security.com/login is not a legitimate PayPal domain.

5) Look for urgent or threatening language

- Phrases like “Urgent”, “Your account has been suspended”, and “Failure to comply within 24 hours” are pressure tactics.

6) Note any mismatched URLs

- Display text says “Verify Your Account Now” but points to a shady domain.

7) Verify presence of spelling or grammar errors

- Message is mostly clean, but tone is slightly off and not professionally structured.

8) Summarize phishing traits found in email

- Spoofed sender domain
- Fake URL masked as secure link
- Urgency and threats used to prompt immediate action
- Slightly suspicious tone and structure