Phishing Email Analysis Report

- **Objective :**

The purpose of this task is to analyze a suspicious email and identify signs that show it is a phishing attempt.

Phishing Email Sample

- **Sender:** DHL support@dhl-delivery-info.com
- **Subject:** Your package delivery is scheduled for today
- **Email Body:**

The email says that a delivery attempt failed due to an address issue and asks the recipient to reschedule the delivery by clicking a link.

- **Phishing Indicators Found**

1. Fake Sender Address

The email claims to be from DHL, but the sender's domain is dhl-delivery-info.com instead of DHL's official domain dhl.com. This shows the sender is trying to impersonate DHL.

2. Suspicious Link

The email includes a link called "Click to Reschedule" that leads to a malicious website and not the official DHL website. This is a common phishing technique used to steal user information.

3. Urgent Message

The email creates urgency by saying there was a delivery problem and asks the user to act quickly. Phishing emails often use urgency to pressure users into clicking links.

4. Generic Greeting

The email starts with "Hello" instead of using the recipient's name. Legitimate companies usually personalize their messages.

Conclusion

This email shows several phishing signs, including a fake sender address, a malicious link, urgent language, and a generic greeting. These indicators confirm that the email is a phishing attempt and should not be trusted.