CYBER SECURITY INTERNSHIP

Task 2 — Phishing Email Analysis

■ Objective:

To analyze a suspicious email and detect phishing indicators.

■ Email Description:

An email claiming to share a PDF document via Google Drive. The visual appearance attempts to mimic Google, with a "Click Here" link and open button.

■■■■■ Observations + Red Flags:

1. Suspicious Sender Email

- Sender address: goog...@protected-download.com

- Not an official Google domain.

2. No Sender Name

- Legitimate Google emails show the sender’s name.

3. Fake Google Drive Preview

- Misleading layout imitating Google UI.

4. Suspicious Link

- Hovering shows unknown URL behind "Click Here".

5. Social Engineering & Urgency

- “Has a document for your review” encourages quick action.

6. Lack of Personalization

- No user name or specific details.

■■ Risk:

May lead to credential theft or malware download.

■ Conclusion:

This email is a phishing attempt designed to trick users into clicking a malicious link.

■ Recommendation:

- Do NOT click suspicious links

- Verify sender domain

- Report phishing emails

- Enable 2FA for Google accounts

End of Report