PHISHING EMAIL DETECTION & AWARENESS REPORT

Cyber Security Internship – Future Interns (2026)
Prepared By: Rohith Rachapudi

1. Executive Summary

Three email samples were analyzed to identify phishing indicators, evaluate authentication mechanisms, and classify risk levels. The assessment focused on technical red flags and psychological manipulation tactics.

Category	Result
Phishing Emails	2
Legitimate Emails	1
Overall Risk Observation	High exposure due to spoofing & urgency tactics

2. Technical Findings

Case 01 – PayPal Verification (Phishing – High)

Domain spoofing (paypa1.com), URL shortener abuse, urgency messaging, SPF/DKIM/DMARC authentication failures. Risk: Credential harvesting.

Case 02 – Microsoft Password Expiration (Phishing – High)

Domain manipulation (micr0soft), fake login link, 12-hour urgency pressure, authentication failures. Risk: Microsoft account compromise.

Case 03 – PayPal Monthly Statement (Legitimate – Safe)

Correct official domain, HTTPS secure link, SPF/DKIM/DMARC authentication passed.

3. Common Phishing Indicators Identified

- Domain variations (1 instead of l, 0 instead of o) - Urgency and fear-based messaging - Suspicious verification links - Authentication failures - Generic greetings

4. Business Impact

Successful phishing attacks may lead to credential theft, financial fraud, account takeover, data leakage, reputational damage, and compliance violations. Phishing primarily exploits human trust and urgency.

5. Employee Awareness Guidelines

DO: Verify sender domains, hover over links, access accounts directly, report suspicious emails.
DO NOT: Click urgent verification links, share passwords or OTPs, ignore authentication warnings.