Phishing Email Detection & Awareness Report

Task 2 – Cyber Security Internship (Future Interns)

---

1. Introduction

Phishing is a type of cyber attack where attackers send fraudulent emails pretending to be from trusted organizations or individuals. The main goal of phishing emails is to steal sensitive information such as login credentials, banking details, or personal data.

This report focuses on identifying phishing emails, understanding common phishing techniques, and spreading awareness to help users stay safe from email-based cyber threats.

---

2. Objective

The objective of this task is to:

- Identify phishing indicators in emails
- Classify emails as Safe, Suspicious, or Phishing
- Explain phishing techniques in simple language
- Provide awareness and prevention guidelines for users

---

3. Tools Used

- Sample phishing emails (public examples)
- Email header analysis (basic understanding)

- Web browser inspection
- Google Docs / MS Word (for documentation)

---

4. What is Phishing?

Phishing is a social engineering attack where attackers trick users into clicking malicious links, downloading infected attachments, or sharing confidential information. These emails often look genuine and create a sense of urgency or fear.

---

5. Common Phishing Indicators

The following indicators help in identifying phishing emails:

- Fake or spoofed sender email address
- Mismatched or shortened links
- Urgent or threatening language
- Requests for passwords, OTPs, or personal data
- Unexpected attachments
- Poor grammar or spelling mistakes

---

6. Phishing Email Example (Analysis)

Example Scenario:

An email claims to be from a bank asking the user to verify their account immediately by clicking a link.

Observed Indicators:

- Sender email does not match the official bank domain
- Link redirects to a fake login page
- Urgent message such as “Account will be blocked”

---

7. Email Classification

Based on analysis, emails can be classified as:

- Safe: Legitimate email from a trusted source
- Suspicious: Email with minor warning signs
- Phishing: Malicious email designed to steal data

Result for Example:

➡️ Classified as: Phishing Email

---

8. Common Phishing Techniques

- Email spoofing
- Fake login pages
- Impersonation of banks or companies
- Urgency-based scams
- Reward or lottery scams

---

9. Prevention & Awareness Guidelines

Users should follow these safety tips to avoid phishing attacks:

- Do not click on unknown or suspicious links
- Always verify sender email addresses
- Never share passwords or OTPs via email
- Enable spam filters and security alerts
- Report suspicious emails immediately

---

10. Conclusion

Phishing emails are a major cybersecurity threat, but they can be detected by carefully analyzing email content, sender details, and links. Awareness and cautious behavior are the most effective defenses against phishing attacks.

This task helped in understanding phishing detection techniques and spreading cybersecurity awareness among users.

---

11. Outcome

A professional phishing detection and awareness report was successfully created, explaining phishing risks, identification methods, and prevention techniques in a clear and user-friendly manner.