PHISHING EMAIL DETECTION & AWARENESS REPORT

Cyber Security Task 2 – 2026
By: Dharani Lk
Internship Program: Future Interns

Introduction

Phishing is a social engineering attack where attackers send fake emails to trick users into revealing sensitive information such as passwords, OTPs, or bank details. These attacks often appear legitimate and create urgency or fear to force quick action.

This report analyses phishing email samples, identifies common phishing indicators, classifies email risk, and provides awareness guidelines to help users avoid phishing attacks.

Objective of the Task

The objectives of this task are:

- To analyse phishing email samples
- To identify common phishing indicators
- To classify emails based on risk level
- To explain phishing attacks in simple language
- To create awareness and prevention guidelines for users

This task focuses on **security awareness**, not hacking.

Tools Used

The following tools were used for analysis:

- Public phishing email samples (GitHub datasets – study purpose)
- Google Message and MX toolbox email Header Analyzer
- MS Word / Google Docs for documentation
- Browser-based URL inspection (without clicking links)

Phishing Email Sample Analysed

Sample Email 1: Account Verification Phishing

Subject: ⚠️ Urgent: Your Account Will Be Locked

Email Body:

Dear User,

We noticed suspicious activity on your account.
To avoid account suspension, please verify your details immediately.

👉 Verify Now: http://secure-account-verify[.]com

Failure to verify within 24 hours will result in permanent account lock.

Regards,
Security Team

Phishing Indicators Identified:

- **Generic greeting (“Dear User”)**
- **Urgency and fear-based language**
- **Suspicious URL not matching any official domain**
- **No official company details**
- **Fake sender identity**

Risk Classification: PHISHING

Sample Email 2: Fake Password Reset Phishing

Subject: Security Alert: Password Reset Required

Email Body:

Hello,

We detected an unauthorized login attempt on your email account.
For your safety, you must reset your password immediately.

Click below to reset your password:
http://mail-security-reset[.]net

If you do not reset your password within 12 hours, your account will be disabled.

Thanks,
Email Support Team

Phishing Indicators Identified:

- **Unknown sender domain**
- **Fake security alert**
- **Short deadline (12 hours)**
- **Suspicious password reset link**
- **No personalization or official branding**

Risk Classification: PHISHING

Sample Email 3: Official Service Notification (Safe Email)

Subject: Your Monthly Account Statement – February 2026

Email Body:

Dear Dharani,

Your monthly account statement for February 2026 is now available.

You can securely view your statement by logging in through our official website or mobile application.

👉 ***https://www.officialbankname.com/login***

If you have any questions, please contact our customer support at support@officialbankname.com or call 1800-XXX-XXXX.

Thank you for choosing Official Bank Name.

Regards,
Customer Support Team
Official Bank Name

Indicators of a Legitimate Email

- **Personalized greeting with real name**
- **Uses official and trusted domain**
- **No urgency or fear-based language**
- **Does not ask for passwords or OTPs**
- **Provides official contact details**
- **Encourages user to log in manually**

Email Risk Classification

Risk Level: SAFE / LEGITIMATE

Reason:
The email follows proper communication standards, uses an official domain, avoids urgent threats, and does not request sensitive information.

How the Attack Works

Attacker sends a fake email pretending to be a trusted service

1. User is pressured using urgency or fear
2. User clicks the malicious link
3. Fake website steals login credentials or personal data
4. Attacker uses stolen data for fraud or account takeover

Prevention & Awareness Guidelines

Do's

- Verify sender email address carefully
- Hover over links before clicking
- Check for spelling or grammar mistakes
- Report suspicious emails to IT/security team
- Use multi-factor authentication (MFA)

Don'ts

- Do not click unknown or urgent links
- Do not share passwords or OTPs via email
- Do not download attachments from unknown senders
- Do not panic when emails create fear

Conclusion

Phishing attacks rely on human error rather than technical flaws. By understanding common phishing indicators and following awareness guidelines, users can protect themselves and their organizations from serious security breaches.

Security awareness is the first line of defence against phishing attacks.