PHISHING EMAIL DETECTION AND AWARENESS REPORT

Cyber Security Task 2: 2026

By: Anushka

Internship By: Future Interns

Introduction

Phishing refers to an attempt to steal sensitive information. This typically includes usernames, passwords, credit card numbers, bank account information, or other important data that can be used or sold. By pretending to be a trustworthy source and making an appealing request, an attacker deceives the victim. This is similar to how a fisherman uses bait to catch a fish.

Objective

- To identify phishing emails using common warning signs.
- To classify phishing emails based on their risk level and potential impact.
- To assess the potential impact of phishing attacks on users and organizations.
- To suggest preventive and mitigation measures against phishing attacks.
- To improve user awareness and response to phishing threats.

Tools Used

- Public email samples
- Browser based URL inspection
- MS word for documentation
- MX toolbox email header analyzer

Phishing email samples analyzed

Sample 1:

From: Security Team <support@paypaI-secure-alerts.com>
To: user@email.com
Subject: ⚠️ Urgent Action Required: Your Account Will Be Suspended

Dear Customer,

We noticed unusual activity on your account. For your protection, we have temporarily limited access to your account.

To restore full access, please verify your information immediately by clicking the link below:

👉 Verify Account Now
http://paypal-secure-verification[.]com/login

If you do not complete this verification within 24 hours, your account will be permanently suspended.

Thank you for helping us keep your account secure.

Sincerely,
PayPal Security Team

Phishing Indicators:

- Email & Sender Indicators
- Message Content Indicators- Generic greeting
- Urgency & Fear Tactics
- Requests for Sensitive Information
- Impersonation Clues

Risk Classification: HIGH

Sample 2:

From: HR Department <hr@company-payrolls.com>
Subject: Action Required: Salary Account Update.

Dear Employee,

Due to recent changes in our payroll system, all employees are required to reconfirm their salary account details.

Please download the attached document and submit the updated information before today 6:00 PM to avoid salary delay.

📎 **Attachment: Salary_Update_Form.html**

Regards,
HR Team

Phishing Indicators:

- Malicious Attachment
- Impersonation
- Urgency Pressure
- Sensitive Information Request
- Potential Impact

Risk Classification: HIGH

Sample 3:

From: IT Support <it-helpdesk@company-loginverify.com>
Subject: New Device Login Detected

Hello,

We detected a new device login to your corporate email account from Delhi, India.

If this was not you, please confirm your activity by clicking the link below:

🔗 **Confirm Login Activity**
https://mail-security-check[.]net/verify

Failure to confirm within 12 hours may result in temporary account restrictions.

IT Support Team

Phishing Indicators:

- Suspicious Login Alert
- Malicious Link
- Authority Impersonation
- Moderate Urgency
- Potential Impact

Risk Classification: MEDIUM

Sample 4:

From: Rewards Team <offers@amaz0n-rewards.net>
Subject: 🎁 Congratulations! You've Been Selected

Dear User,

Congratulations! You have been selected to receive a free gift voucher worth ₹5,000 as part of our customer appreciation program.

To claim your reward, click the link below and complete a short form:

👉 Claim Your Reward
http://amaz0n-rewards[.]net/claim

Offer valid for today only.

Thank you,
Rewards Team

Phishing Indicators:

- Too-Good-To-Be-True Offer
- Fake Sender Domain
- No Immediate Sensitive Data Request
- Basic Social Engineering
- Potential Impact

Risk Classification: LOW

Sample 5:

From: SBI-UPI Alert <sbi-upi@secure-payments.in>
Subject: UPI Transaction Failed

Dear Customer,

Your UPI transaction of ₹4,850 has failed due to incomplete KYC.

To avoid account blockage, please update your KYC immediately using the link below:

🔗 **Update KYC Now**
https://sbi-kyc-update[.]in

If not updated within 2 hours, UPI services will be temporarily suspended.

— SBI UPI Team

Phishing Indicators:

- Financial & Banking Context
- Impersonation of Trusted Bank
- Credential / OTP Harvesting
- Extreme Urgency
- Potential Impact

Risk Classification: HIGH