PHISHING EMAIL DETECTION & AWARENESS SYSTEM

Cyber security Internship -TASK 2

Internship Program: Future Interns

Submitted By: shashank

Date: 28 February 2026

Introduction

Phishing is a type of cyberattack in which attackers impersonate trusted organizations to trick users into revealing sensitive information such as passwords, banking credentials, OTPs, or personal data. These attacks are commonly delivered through email and rely heavily on social engineering techniques such as urgency, fear, and reward-based manipulation.

The objective of this task is to analyze sample emails, identify phishing indicators, classify them into Safe, Suspicious, or Phishing categories, and provide awareness and prevention guidelines.

Tools Used

- Sample phishing emails (simulated)
- Email content analysis
- Link inspection method
- Domain verification concept
- MS Word for documentation

Email Analysis & Classification

Email 1 – Phishing

Subject: Urgent: Your Bank Account Will Be Suspended

From: support@hdfc-alert-demo.com

Email Content:

Dear Customer,
We detected unusual activity in your HDFC Bank account.

Your account will be suspended within 24 hours.

Click below to verify immediately:

http://hdfc-verify-demo.com

Indicators Identified:

- Fake domain (not official hdfcbank.com)
- Urgency & Fear tactics.
- Generic greeting.
- Suspicious link.

Risk Level: High

Classification: Phishing Email.

Email 2 -Suspicious

Subject: Congratulations! You Won ₹5,00,000

From: rewardcenter-demo@gmail.com

Email Content:

Congratulations!

You have been selected as a winner of ₹5,00,000 in our lottery program. Send your Adhaar number and bank details to claim your reward.

Indicators Identified:

- Unrealistic reward offer
- Non-official sender (Gmail)
- Request for sensitive personal information
- No verification of organization

Risk Level: Medium

Classification: Suspicious Email

Email 3 – Safe

Subject: Monthly Account Statement – January

From: noreply@hdfcbank.com

Email Content:

Dear Mr. Sharma,

Your January account statement is now available. Please log in through the official HDFC Bank Net Banking portal to view your statement.

Indicators Observed:

- Official domain (hdfcbank.com)
- Professional tone
- No urgency or threats
- No request for sensitive information
- No suspicious links.

Risk Level: Low

Classification: Safe Email

Phishing Techniques Identified

Attackers often use psychological tricks and technical methods to trick users. The following techniques were identified during analysis:

- **Domain Spoofing**: Using fake or similar-looking email addresses to impersonate a trusted source.
- **Urgency / Fear Tactics**: Messages that create panic, e.g., “Account will be suspended within 24 hours.”
- **Greed / Reward Scams**: Fake lottery or prize messages to lure users.
- **Suspicious Links**: URLs that do not match official domains or redirect to malicious sites.
- **Social Engineering**: Manipulating user behaviour through emotions or trust.

Risk Impact Explanation

If phishing emails are successful, the potential risks include:

- **Financial Fraud**: Unauthorized transactions or account compromise.
- **Identity Theft**: Attackers may steal personal information.
- **Credential Compromise**: Login details may be harvested.
- **Malware Infection**: Malicious links or attachments may infect devices.
- **Organizational Data Breach**: Sensitive company data can be exposed.

Prevention & Awareness Guidelines

For Individuals:

- Verify the sender’s email address carefully.
- Hover over links before clicking to check the actual URL.
- Never share OTPs, passwords, or banking details via email.

- Enable Two-Factor Authentication (2FA) wherever possible.
- Avoid downloading attachments from unknown sources.
- Report suspicious emails to IT/security teams.

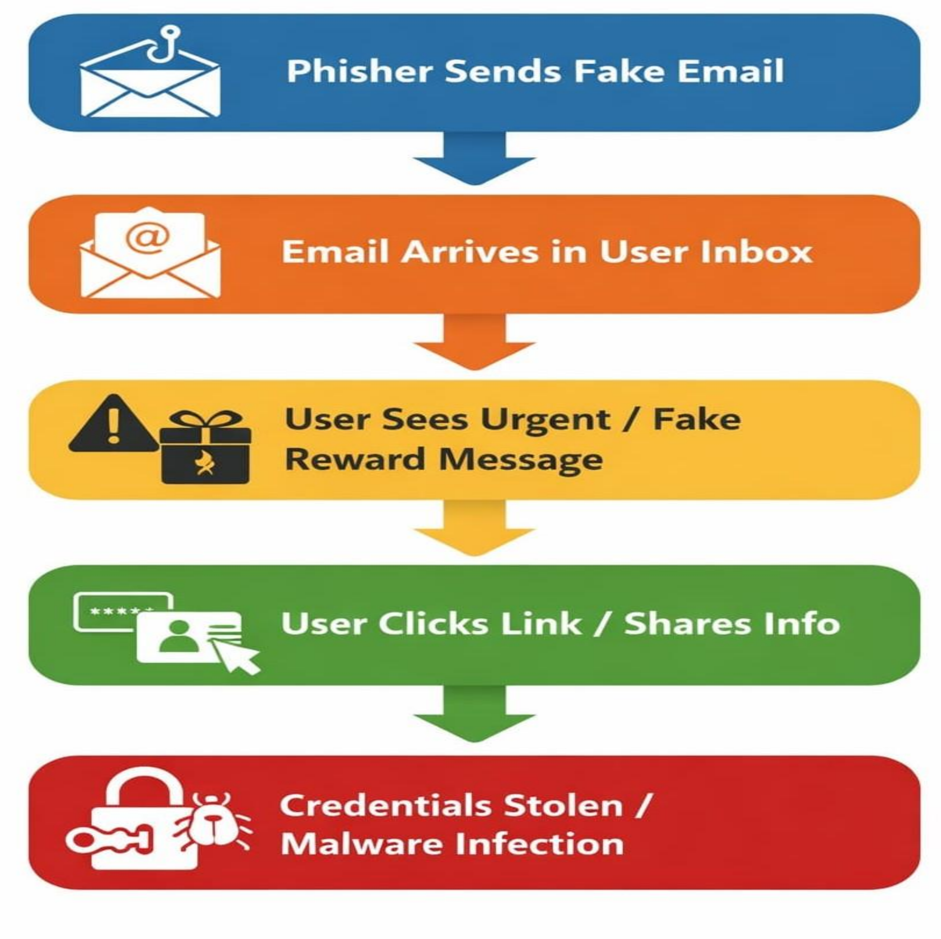
For Organizations:

- Conduct regular phishing awareness training for employees.
- Implement email filtering and spam detection systems.
- Use SPF, DKIM, and DMARC email authentication policies.
- Perform simulated phishing exercises to test employees.
- Maintain endpoint protection and monitor unusual activities.

Table of Email Classification

Email	Subject	From	Indicators Identified	Risk level	Classification
Email1	Urgent: Your HDFC Bank Account will be Suspended	support@hdfc-alert-demo.com	Fake domain, urgency/fear, generic greeting, suspicious link.	High	Phishing
Email 2	Congratulations! You Won ₹5,00,000	Rewardcenter-demo@gmail.com	Unrealistic reward, non-official sender, requests sensitive info, no org verification.	Medium	Suspicious
Email 3	Monthly Account statement - January	noreply@hdfcbank.com	Official domain, professional tone, no urgency, no sensitive info requested.	Low	Safe

Phishing Process Flowchart


Phisher Sends Fake Email
Email Arrives in User Inbox
@
User Sees Urgent / Fake Reward Message
User Clicks Link / Shares Info
*****
Credentials Stolen / Malware Infection

Conclusion:

Phishing attacks remain one of the most common cybersecurity threats. By identifying suspicious indicators such as fake domains, urgency tactics, and requests for sensitive information, users can reduce the risk of cyber fraud. Awareness, preventive measures, and technical controls are essential for maintaining cybersecurity hygiene.