NAME: COLLINS KARURI KING'ORI

CIN ID: FIT/JAN26/CS5913

Task 2:phishing Email detection & Awareness system

Introduction

Phishing is a cyberattack technique where attackers impersonate trusted organizations or individuals to trick users into revealing sensitive information such as passwords, bank details, or personal data.

This project analyzes phishing email samples to identify malicious indicators, classify email threats, and provide awareness guidelines to prevent phishing attacks.

2. Tools Used

- Sample phishing email datasets
- Email header analyzer
- Browser inspection tools
- VirusTotal (for link analysis)
- SPF/DKIM/DMARC header checking

3. Email Analysis

🔎 **Sample Email 1**

Subject: Urgent: Your Account Has Been Suspended
Sender: support-paypal@secure-verification-login.com

Indicators Identified:

- Spoofed sender email address
- Urgent language ("Urgent", "Immediately")
- Suspicious domain (not paypal.com)
- Contains login link
- Generic greeting ("Dear Customer")

Classification:

✅ Phishing Email

Risk Level:

High Risk – Credential theft attempt

🔎 **Sample Email 2**

Subject: Staff Meeting Reminder
Sender: hr@companyname.com

Indicators:

- Legitimate domain
- No suspicious links
- Personalized greeting
- No urgency or threats

Classification:

✅ Safe Email

4. Common Phishing Indicators

- Spoofed sender address
- Misspelled domain names
- Urgent or threatening language
- Suspicious links or attachments
- Generic greetings
- Requests for sensitive information

5. Phishing Techniques Explained

1. Email Spoofing

Attackers fake sender email addresses to appear legitimate.

2. Link Manipulation

Malicious links redirect users to fake login pages.

3. Social Engineering

Attackers create fear, urgency, or curiosity to manipulate victims.

4. Attachment-Based Malware

Malicious files infect systems when opened.

---

6. Prevention & Awareness Guidelines

- Always verify sender email addresses
- Hover over links before clicking
- Do not share passwords via email

- Enable Multi-Factor Authentication (MFA)
- Report suspicious emails to IT
- Use email filtering and anti-phishing tool

7. Conclusion

Phishing remains one of the most common cyber threats. By identifying phishing indicators and promoting user awareness, organizations can significantly reduce the risk of credential theft and financial loss.