Phishing Email Detection & Awareness System

Objective

The objective of this project is to identify phishing emails by analyzing email characteristics such as sender address, subject content, and embedded links. The project also focuses on educating users by providing awareness messages and prevention guidelines to reduce email-based cyber threats.

Tools & Technologies Used

- Python
- Pandas
- Phishing email samples (public datasets)
- Command Prompt
- Google Docs / MS Word

Methodology

1. Collected sample phishing and legitimate emails.
2. Extracted key indicators such as suspicious links, spoofed sender domains, and urgent keywords.
3. Developed a Python-based rule-based detection system.
4. Classified emails as Safe, Suspicious, or Phishing.
5. Generated awareness messages explaining risks and prevention steps.

Phishing Indicators Identified

- Spoofed or fake sender domains
- Presence of malicious URLs
- Urgent or threatening language
- Requests for sensitive information

Sample Email Analysis

Subject	Sender	Classification
Verify your account	fake@xyz.com	Phishing
Meeting Notes	boss@trusted.com	Safe
Password Reset Required	alert@bank.com	Suspicious

Risk Explanation

Phishing emails attempt to trick users into revealing sensitive information such as login credentials or financial data. Successful phishing attacks can lead to identity theft, financial loss, and organizational breaches.

Prevention & Awareness Guidelines

- Do not click unknown or suspicious links.
- Always verify the sender’s email address.
- Avoid sharing sensitive information via email.
- Report phishing emails to the security team.
- Use updated security software.

Conclusion

This project demonstrates a simple yet effective approach to detecting phishing emails and raising awareness among users. It helps users understand common phishing techniques and encourages safe email practices.