Final Year Project Proposal

Student Information:

|  |  |
| --- | --- |
| Name: Ali Haider | Student ID: Fa-21/BS DFCS/028 |
| Contact Information: +923154493412 | Supervisor: |

Project Title:

Automate Phishing Detection System

Project Description:

Objective: We will focus on **rule-based detection.** Phishing attacks are a major cybersecurity threat, where attackers trick users into providing sensitive information like passwords, credit card details, and personal data. This project aims to develop an **automated phishing detection system** using **rule-based analysis, blacklist verification, and heuristic techniques** to identify and prevent phishing attempts.

The system will analyze incoming emails, URLs, and website content based on predefined security rules and patterns. It will flag suspicious content, notify users, and provide recommendations to prevent phishing attacks. The project will be implemented as a **browser extension, email filter, or standalone application** to enhance user security.

### ****Objectives:****

1. **Automate Phishing Detection:** Develop a system that scans emails, messages, and URLs to identify phishing attempts based on predefined rules.
2. **Rule-Based Analysis:** Implement keyword filtering, domain reputation checks, and URL analysis to detect suspicious links.
3. **Blacklist & Whitelist Approach:** Maintain a database of known phishing websites and legitimate domains to compare incoming URLs.
4. **Heuristic-Based Detection:** Use common phishing indicators such as **misspelled domains, excessive use of urgent language (e.g., "Your account will be locked!"), and hidden links** to detect phishing attempts.
5. **User Alert System:** Display real-time alerts or warnings when a phishing attempt is detected.

Relevance to Degree Program:

"Automate Phishing Detection System," is highly relevant to a cybersecurity degree as it focuses on threat detection and prevention, a core aspect of cybersecurity. It helps protect users from phishing attacks by analyzing emails, URLs, and website content using rule-based detection and heuristics. This project aligns with key cybersecurity domains such as network security, incident response, and web security, making it valuable for roles like SOC Analyst, Cybersecurity Engineer, and GRC Analyst.

Proposed Methodology: The proposed methodology for the Automated Phishing Detection System follows a structured approach to effectively identify and mitigate phishing threats. First, a requirement analysis is conducted to define the scope, detection techniques, and deployment method. Next, data collection and preprocessing involve gathering phishing and legitimate URLs/emails from sources like PhishTank and analyzing key features such as domain reputation, email headers, and suspicious keywords. The detection phase employs a rule-based approach, including URL analysis (checking for misspelled domains, HTTPS presence, and blacklist verification), content filtering (flagging phishing-related keywords), and email header inspection (detecting spoofed senders and obfuscation techniques). The system is then developed using Python, JavaScript, or PHP and integrated into a suitable platform. Finally, the system is deployed, providing real-time alerts to users while allowing them to report phishing attempts, enhancing both security awareness and system effectiveness.

URL-Based Features (Website Analysis)

* URL Length: Long URLs are suspicious.
* Number of Dots (.): More subdomains may indicate phishing.
* Presence of "@" or "-": Used to trick users.
* Use of HTTP vs. HTTPS: Legitimate sites use HTTPS.
* Presence of IP Address Instead of Domain: Phishing sites often use raw IPs.
* Domain Age: Newly registered domains can be suspicious.
* Blacklisted Domains: Check if the domain is in a phishing database.

|  |  |
| --- | --- |
| Date of Submission: 23-03-2025 | Signature: Ali Haider |
|  |  |
| Supervisor Remarks: | [Accepted] / [Rejected] |
|  | |