WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Unified Multilingual Cyber Security Awareness and Scam Prevention Web Application

Khatija Dalwai[1], Pragati Ravi Gangoji[1], Ayan Chajju[1], Omkar Shetty[1], Prof. Santosh Patil[2], Mr. Gajendra Deshpande[2]

[1]UG Students, Department of Computer Science and Engineering, Angadi Institute of Technology and Management, Belagavi, India
[2]Assistant Professors, Department of Computer Science and Engineering, Angadi Institute of Technology and Management, Belagavi, India

ABSTRACT

Cyber crimes such as phishing attacks, fake URLs, fraudulent phone calls, OTP scams, and password breaches have increased rapidly with the growth of internet usage and digital services. Most victims fall prey to these attacks due to lack of cyber awareness and the absence of simple, trustworthy tools for prevention. Existing cyber security solutions are scattered across multiple applications, often require user login, and pose privacy risks.

This paper presents SECURO, a unified multilingual cyber security awareness and scam prevention web application that integrates cyber crime education with real-time security tools in a single platform. The proposed system provides phishing URL detection, phone number checking, password strength analysis, and email safety guidelines without requiring user authentication.

The application supports English, Hindi, and Kannada to improve accessibility for Indian users. Developed using modern web technologies and a serverless architecture powered by the Google Gemini API, SECURO follows a privacy-first approach by ensuring that no sensitive user data is stored. The system aims to improve cyber security awareness while providing reliable scam prevention for common users.

Keywords: Cyber Security Awareness, Scam Prevention, Phishing Detection, Multilingual Web Application, Privacy-Focused Design, Serverless Architecture

1. Introduction

The rapid advancement of digital technologies has significantly increased dependence on online platforms for communication, banking, education, and daily activities. Along with these benefits, cyber crimes such as phishing emails, malicious websites, fake phone calls, OTP frauds, and social engineering attacks have become increasingly common. Non-technical users are often unaware of these threats and are unable to identify scams in real time.

Although various cyber security tools and awareness platforms exist, most of them operate independently and require application downloads or user authentication. Awareness-based platforms lack practical tools, while prevention-based tools fail to educate users. This gap creates the need for a unified solution that combines awareness and prevention in a secure and user-friendly manner.

2. Problem Statement

The current cyber security ecosystem faces several challenges that reduce its effectiveness for common users. Security tools are distributed across multiple platforms, making it difficult for users to identify reliable solutions. Many applications require login and collect sensitive personal data, which raises serious privacy concerns. Additionally, limited availability of regional language support and the separation of cyber awareness content from real-time prevention tools reduce accessibility and usability. As a result, users remain vulnerable to cyber attacks despite the availability of multiple security solutions.

3. Objectives of the Project

The primary objective of the proposed system is to provide comprehensive cyber crime awareness in a simple and easily understandable manner, especially for non-technical users. The system aims to offer real-time scam prevention utilities that can assist users in identifying threats such as phishing URLs, suspicious phone numbers, and weak passwords. A key goal is to eliminate data privacy risks by avoiding any form of user authentication, ensuring that the platform remains fully privacy-focused. Additionally, the system intends to support multiple regional languages to make cyber safety accessible

to a diverse audience across India. Overall, the project seeks to integrate both awareness and security tools into a single unified platform, enabling users to learn about cyber threats while simultaneously protecting themselves from them.

4. Existing System

Existing cyber security solutions include phishing URL checkers, password analyzers, scam-detection mobile applications, and cyber awareness websites. However, these systems are fragmented, often require login, and may store user data externally. Most tools are available only in English and lack accessibility for regional language users. Additionally, awareness platforms do not provide practical scam detection features.

5. Proposed System

The proposed system, SECURO, is a unified multilingual web-based cyber security awareness and scam prevention application. It integrates awareness content with practical security tools while ensuring complete user privacy.

Features of SECURO

1. Cyber crime awareness module
2. Phishing URL scanner
3. Phone number checker
4. Password strength analyzer
5. Gmail safety guidelines
6. Multilingual support (English, Hindi, Kannada)
7. No login or external data storage

6. System Architecture

The system follows a client-side and serverless architecture.

1. **Frontend:**
React 19, TypeScript, Tailwind CSS, HTML, Lucide Icons
2. **Backend:**
Serverless architecture using Google Gemini API
3. **Storage:**
Browser-based LocalStorage
4. **Development Tools:**

Node.js, Vite, JSON configuration files

7. Module Description

7.1 Cyber Crime Awareness Module

Provides information on phishing scams, OTP frauds, fake calls, and social media scams along with recommended recovery steps.

7.2 Phishing URL Scanner

Analyzes URLs to identify potentially malicious or unsafe links.

7.3 Phone Number Checker

Helps users verify suspicious phone numbers commonly associated with scam activities.

7.4 Password Strength Analyzer

Evaluates password strength locally within the browser without storing user data.

7.5 Gmail Safety Guidelines

Provides best practices to secure Gmail accounts against unauthorized access.

7.6 Multilingual Interface

Allows users to switch between English, Hindi, and Kannada to improve usability.

8. Methodology

SECURO uses a privacy-first methodology. All inputs are processed in real time using serverless APIs, and results are displayed instantly. No user data is stored on external servers. The system is designed to be lightweight, secure, and accessible to users with minimal technical knowledge.

9. Results

The proposed system successfully demonstrates the ability to identify suspicious phishing URLs and assist users in evaluating the strength of their passwords in real time. By integrating awareness content with practical security tools, the application enhances cyber crime awareness among users and helps them understand common scam techniques. The multilingual support feature improves accessibility for users from different linguistic backgrounds, making the platform more inclusive and user friendly. Additionally, the privacy-first design ensures that no sensitive user data is stored or shared, thereby maintaining user trust and providing a secure and reliable cyber safety solution.

10. Comparative Analysis

Feature	**Existing Systems**	**SECURO**
Integrated tools	No	Yes
Login required	Yes	No
Data storage	External	Local only
Multilingual support	No	Yes
Awareness + Prevention	Partial	Complete

11. Conclusion

SECURO effectively addresses the limitations of existing cyber security tools by providing a unified, multilingual, and privacy-focused platform. By integrating awareness and prevention features, the system empowers users to protect themselves from cyber threats. It is especially beneficial for non-technical and regional language users.

12. Future Scope

The proposed system can be further enhanced in several meaningful ways. One major improvement is the addition of more Indian regional languages to increase accessibility for a wider demographic. Advanced AI-based scam message detection can be integrated to automatically identify fraudulent patterns in real-time communication. The system can also be expanded to analyze suspicious SMS and email content, providing users with instant risk assessments. Furthermore, developing a browser extension would allow users to receive scam warnings directly while browsing. Finally, creating a dedicated mobile application would improve usability and provide on-the-go protection for users across different devices.

References

Google. (2024). ***Google Safe Browsing: Protecting Users from Harmful Websites****. Google Security Documentation.*

Open Web Application Security Project (OWASP). (2023). ***OWASP Web Application Security Testing Guide****. OWASP Foundation.*

Open Web Application Security Project (OWASP). (2023). ***Phishing Attack Prevention and Detection Techniques****. OWASP Foundation.*

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). ***A survey of phishing email filtering techniques****.* IEEE Communications Surveys & Tutorials, *15(4), 2070–2090.*

Sahoo, D., Liu, C., & Hoi, S. C. H. (2020). ***Malicious URL detection using machine learning: A survey****.* ACM Computing Surveys, *53(4), 1–42.*

Fette, I., Sadeh, N., & Tomasic, A. (2007). ***Learning to detect phishing emails***. Proceedings of the 16th International World Wide Web Conference, *Banff, Canada.*

Google. (2024). ***Gmail Security and Account Protection Best Practices***. *Google Account Safety Center*.

Federal Trade Commission (FTC). (2023). ***Consumer Information on Phone Call and SMS Scams***. *FTC Reports.*

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). ***Advanced social engineering attacks***. Journal of Information Security and Applications, *22, 113–122.*

Government of India. (2023). ***Cyber Crime Awareness and Online Safety Guidelines***. *Ministry of Home Affairs, India*.

Chiew, K. L., Chang, E. H., Sze, S. N., & Tiong, W. K. (2019). ***A survey of phishing attacks: Their types, vectors, and technical approaches***. Expert Systems with Applications, *106, 1–20.*