A Study of Cybersecurity Awareness Among Digitally Less Literate People with A Community-Driven Fraud Reporting Application

Chindhe Snehal Sunil[1], Jadhav Gauri Ganesh[2], Cholke Pranjal Vasant[3], Ghuge Kaveri Pandurang[4], Dighe Snehal Valmik[5], Sunil Mahajan[6]

[1,2,3,4,5]*F.Y.M.Sc. (Computer Science), MIT Arts, Commerce and Science College, Alandi (D), Pune, Maharashtra, India*

[6]*Associate Professor, Department of Electronics, MIT Arts, Commerce and Science College, Alandi (D), Pune, Maharashtra, India*

doi.org/10.64643/ijirt.208495-459

***Abstract*—The widespread use of mobile phones for payments, social media, online shopping, and banking has significantly increased exposure to cyber fraud, particularly among individuals with limited digital literacy. Such individuals often struggle to distinguish genuine communication from fraudulent attempts, making them vulnerable to impersonation calls, phishing links, and requests for sensitive information such as One-Time Passwords (OTPs), UPI PINs, or bank details. This research examines the level of cybersecurity awareness among digitally less literate people, focusing on common fraud scenarios encountered in daily life, including fake calls, OTP fraud, UPI fraud, and impersonation of officials or company representatives. As part of this study, a community-driven mobile application is proposed to assist users in identifying suspicious phone numbers. The application allows users to check whether a number has been previously reported for fraud, submit their own reports with supporting details, and view administrator-verified warnings when a number accumulates multiple approved reports. The application further educates users through simple, visual explanations of common fraud types and appropriate protective responses.**

To evaluate the effectiveness of this approach, participants' awareness levels are assessed through a pre-intervention questionnaire, followed by exposure to the application and its awareness material, and a subsequent post-intervention assessment. Comparing the two results enables measurement of improvement in participants' ability to recognize and respond to suspicious situations. This study aims to highlight the challenges faced by digitally less literate individuals and to demonstrate the potential of a simple, accessible application in strengthening their preparedness against cyber fraud.

Index Terms*—*Cybersecurity Awareness, Digital Literacy, OTP Fraud, UPI Fraud, Phishing, Fraud Reporting Application, Community Reporting

I. INTRODUCTION

Digital technology has become deeply embedded in everyday routines across India, from mobile banking Unified Payments Interface (UPI) transactions to social media communication and e-governance services. This rapid expansion of connectivity has brought undeniable convenience, but it has simultaneously opened new avenues for exploitation. Cybercriminals increasingly rely not on breaking technical safeguards but on manipulating human trust impersonating bank officials, government agents, or delivery personnel; sending fraudulent links disguised as legitimate notifications; and pressuring victims into revealing One-Time Passwords (OTPs), UPI PINs, or banking credentials.

These tactics succeed disproportionately against users who are digitally less literate: individuals who may operate a smartphone competently enough for calls, messaging, or payments, yet lack the conceptual understanding needed to recognize manipulation, verify a sender's authenticity, or judge when a request for information is illegitimate. This vulnerability is not confined to any single age group. While much existing research has concentrated on older adults as the primary at-risk population, digitally less literate users span a much broader demographic first-time smartphone owners, individuals with limited formal

education, rural users with recent internet access, and people who adopted digital payment systems out of necessity rather than familiarity.

For this group, the gap is rarely one of access; India's digital payment infrastructure has expanded rapidly through UPI and related services. The gap instead lies in the ability to convert access into safe, informed use the capacity to pause, question, and verify before responding to a fraudulent call or message. National-level fraud statistics reinforce the scale of the problem: UPI transaction fraud in India has risen sharply in recent years even as transaction volumes grew, indicating that expanding adoption has not been matched by a proportionate rise in user preparedness.

A recurring theme across this body of research is that awareness alone does not guarantee safe behaviour; individuals who report having heard of scams frequently continue to trust unsolicited calls, click unfamiliar links, or share sensitive details when pressured. Existing interventions to address this problem have largely taken the form of one-time training sessions, government advisories, or general digital literacy campaigns. While these approaches contribute to baseline awareness, they tend to be static, delivered once, and disconnected from the real-time, evolving nature of fraud tactics. They also rarely give ordinary users a practical tool to act on suspicion in the moment for instance, when receiving an unknown call that feels suspicious but cannot be immediately confirmed as fraudulent.

This study addresses that practical gap by proposing a community-driven fraud reporting application designed specifically with digitally less literate users in mind. The application allows users to check whether a phone number has previously been reported for fraudulent activity, submit their own reports with supporting details, and receive administrator-verified warnings once a number accumulates a threshold of approved reports. Alongside this reporting mechanism, the application delivers simple, visual educational content explaining common fraud types fake calls, OTP fraud, UPI fraud, and impersonation scams and the appropriate protective response to each. By combining crowd-sourced verification with accessible awareness material, the tool aims to convert collective user experience into a shared early-warning system, reducing reliance on individual judgment alone. To assess whether this combined approach meaningfully improves user preparedness, the study adopts a pre-test and post-test design: participants' baseline cybersecurity awareness is measured through a structured questionnaire, followed by exposure to the application and its educational content, and a subsequent assessment to measure change. This design allows the study to move beyond simply documenting the existence of an awareness gap a well-established finding in prior literature toward evaluating whether a low-cost, community-based digital tool can produce measurable improvement in a population that formal training programmes have historically struggled to reach.

II. LITERATURE REVIEW

Previous research has shown that digital literacy does not just mean being able to operate a mobile phone or computer. Digital literacy includes the ability to identify online threats, distinguish genuine messages from fraudulent ones, recognize suspicious links, and follow safe digital practices [2], [3]. People with low digital literacy may have difficulty identifying phishing messages, fake calls, impersonation, and financial scams. This issue is important in India because the use of digital technology such as UPI, mobile banking, and online shopping has increased significantly, but not all users have improved their cybersecurity knowledge to the same extent.

Cyber fraud does not happen only because of weaknesses in technology; frequently, the fraudster manipulates the user psychologically for example, by claiming to call from a bank, warning that KYC will be deactivated, or urgently requesting an OTP. The fraudster creates fear, urgency, or trust in the user. Common UPI-related frauds include phishing links, fake calls, impersonation, OTP fraud, UPI PIN fraud, and fraudulent payment requests [4], [10], [11]. Using UPI safely requires more than knowing how to make payments; users should also know how to identify suspicious calls, messages, and payment requests, since cyber fraud often works by exploiting people's trust.

An important finding from previous research is that awareness does not always lead to safe behaviour. A user may know that an OTP should never be shared, but may still disclose it when a fraudster impersonates a bank official and creates fear by claiming the account will be blocked. This indicates that knowledge alone

is insufficient when users are unable to translate that knowledge into the right action under pressure. Therefore, previous studies suggest that training using practical examples, demonstrations, and real-life situations can help users identify suspicious situations more reliably [5], [6], [12], [13].

Knowing about fraud is not always enough; users also need to know how to respond. Mechanisms exist with banks, payment services, and government agencies for reporting fraud after it occurs, but some people do not report it, owing to not knowing where or how to report, the apparent complexity of the procedure, or a lack of information [7], [8], [9]. This creates a gap in which an individual's experience with fraud fails to provide useful warning information to other members of the community.

A community-based approach addresses this gap by making one user's experience useful for other users. For example, if multiple users independently report the same phone number as suspicious, the accumulated reports can provide an early warning to other community members. However, since user-generated reports may not always be accurate, administrator verification is necessary before displaying an official warning community reporting can create useful knowledge, but it must be checked for reliability.

Overall, prior studies have found that UPI fraud, phishing, OTP fraud, impersonation, and social engineering are common cyber threats, and that practical, example-based training can help users identify them [1], [14], [15]. Studies on fraud reporting have separately shown that many users face difficulties when reporting fraud. These topics have primarily been studied in isolation, and comparatively less attention has been given to integrating awareness education, risk analysis, and community-verified reporting into a single system specifically designed for digitally less literate users the gap this research addresses.

III. PROPOSED METHODOLOGY

A. Research Design

A design-and-development based research approach has been used in this research. The objective is to study cybersecurity awareness among digitally less-literate people and to develop a simple application that helps them identify and respond to cyber fraud. Although people with low digital literacy use smartphones, digital payments, online banking, and messaging applications, they may not necessarily have sufficient knowledge about cybersecurity threats, and may therefore face difficulties in identifying fraudulent phone calls, fake customer-care representatives, phishing links, OTP-related scams, UPI/payment fraud, and requests asking for confidential information.

The proposed research therefore includes two main aspects: first, studying cybersecurity awareness among the target users and the difficulties they face; and second, developing a user-friendly cybersecurity awareness and fraud-assistance web application based on these identified requirements.

The overall process is divided into the following stages: Problem Identification → Literature Review → Requirement Identification → System Design → Application Development → Technical Testing → Database Integration → User Evaluation → Data Analysis → Conclusion. The application development stage includes frontend development, backend development, database integration, API development, and technical testing. User evaluation is a subsequent research stage intended to determine whether the application helps improve cybersecurity awareness.

B. Problem Identification

This research begins with identifying the real-world cybersecurity problem faced by people with low digital literacy. Many digital frauds rely on social engineering rather than sophisticated technical attacks: fraudsters contact users through phone calls, messages, social media, or payment platforms and attempt to obtain sensitive information such as OTPs, bank details, UPI credentials, passwords, or personal information, or ask users to open suspicious links.

For digitally less-literate users, such situations can be difficult to identify because fraudulent communication may appear to originate from a bank, government organization, customer-care service, delivery company, or other trusted source. This research therefore identifies the need for a simple system that can analyze suspicious information, explain possible warning signs, provide cybersecurity awareness material, and guide users toward appropriate actions.

C. Requirement Analysis

The requirements were divided into functional and non-functional requirements, summarized in Table I.

TABLE I. FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

#	Functional Requirements	Non-Functional Requirements
1	Provide a simple home screen	Be simple to use
2	Provide language selection and an Easy Mode	Be easy to understand
3	Provide voice assistance / voice input	Be responsive and beginner-friendly
4	Allow users to check suspicious messages	Be maintainable
5	Allow analysis of suspicious screenshots	Be modular
6	Allow verification of suspicious phone numbers	Be scalable for future enhancement
7	Allow verification of suspicious URLs	Follow privacy-conscious and responsible reporting practices
8	Display risk score, warning signs, explanation and recommended action	—
9	Allow users to submit a suspected fraud report	—
10	Provide an evidence checklist and guidance	—
11	Provide cybersecurity awareness and learning content	—
12	Provide an interactive quiz	—
13	Provide help and official cybercrime/safety resources	—
14	Provide trusted-person assistance	—
15	Validate user inputs and uploaded information	—
16	Provide confirmation and error messages	—
17	Store application data using the backend database	—

D. Application Modules

The developed Digital Safety Assistant contains multiple modules designed to help users identify, understand, and respond to cyber-fraud situations, summarized in Table II.

TABLE II. APPLICATION MODULES

Module	Function
Home	Main entry point providing simple access to the major safety features: Check Something, Risk Analysis, Report Fraud, Awareness/Learning, Help and safety resources
Language and Easy Mode	Provides language support, an Easy Mode, and voice assistance/voice input to improve accessibility
Check Something	Allows users to submit suspicious messages, screenshots, phone numbers, or URLs for analysis
Message and Screenshot Analysis	Checks entered or pasted messages and screenshots for suspicious indicators and presents results in simple language
Phone Number Verification	Validates and checks a suspicious phone number, returning an appropriate result
URL Verification	Analyzes a suspicious website address for suspicious indicators and provides a risk score and explanation
Risk Analysis	Presents a risk score, risk level, warning signs, explanation, and recommended action
Report Fraud	Allows users to submit information about a suspected cyber-fraud incident, with input validation and an evidence checklist
Awareness and Learning Hub	Provides cybersecurity education on OTP fraud, phishing, fake calls, payment fraud, suspicious links, impersonation, and safe practices
Interactive Quiz	Provides a simple quiz to reinforce learning through scenario-based questions
Help and Official Resources	Provides guidance and official safety resources for cybercrime reporting
Trusted Person	Allows users to involve a trusted individual when dealing with a suspicious situation

The general processing flow within the Check Something module is: User Input → Validation →

Analysis → Risk Score → Warning Signs → Explanation → Recommended Action. A low-risk result does not guarantee that a message, phone number, or URL is completely safe; risk analysis is based on programmed rules and available information rather than a legal determination of fraud. Similarly, submitted reports do not automatically classify a person or phone number as legally fraudulent a proper verification and moderation mechanism is required before a warning is shared with other users.

E. Data Design

The current implementation uses a relational database through the Spring Boot backend. The database design contains records required for fraud reporting, awareness content, trusted-person information, and other application data. Appropriate validation and responsible moderation are required for user-generated fraud information. Table III summarizes the primary fields used for fraud reports.

TABLE III. FRAUD REPORT DATA FIELDS

Field	Description
Report ID	Unique identifier
Phone Number	Number associated with a report
Fraud Type	Category of suspected fraud
Description	User-provided explanation
Report Count	Number of reports associated with the number
Risk Level	Example: Low, Medium, High
Status	Example: Reported, under review, Verified
Date	Date of report

F. Research Evaluation Method

After completion of application development and technical testing, the application can be evaluated with participants from the intended user group using a pre-test/post-test approach:

1. Pre-Test: Participants answer questions measuring existing cybersecurity awareness across topics such as OTP safety, phishing, fake calls, suspicious links, online payment safety, and reporting cyber fraud.
2. Application Use: Participants use the application and explore Check Something, Message Analysis, Screenshot Analysis, Phone Verification, URL Verification, Risk Analysis, the Awareness Hub, Report Fraud, the Quiz, and Help/Safety Resources.
3. Post-Test: Participants answer a similar set of awareness questions after using the application.
4. Usability Evaluation: Participants rate statements on a five-point scale (Strongly Disagree to Strongly Agree), such as “The application was easy to understand” and “I understand better why I should not share an OTP.”

IV. IMPLEMENTATION

A. Development Technology

The Digital Safety Assistant was developed as a Java-based web application using Spring Boot for the backend and HTML, CSS, and JavaScript for the frontend interface. The main technologies used are Java, Spring Boot, Spring Web/REST functionality, Spring Data JPA, Maven, MySQL, HTML, CSS, and JavaScript. The backend is organized into controllers, services, repositories, and models/entities to keep the application modular and maintainable. Spring Boot provides the web application framework and embedded server environment, while Spring Data JPA is used for database access and object-relational mapping with MySQL as the relational database.

B. Current Data Implementation

The current implementation uses MySQL as the relational database instead of relying only on local or sample repository data. The Spring Boot backend communicates with the database through Spring Data JPA. Sample records may be used during testing, but such sample data is used only to verify functionality and should not be presented as evidence that a real-world phone number, person, or organization is fraudulent.

C. Backend / API Implementation

The backend provides application services and API endpoints for communication between the web interface and the Java Spring Boot application. This separation between the frontend and backend allows the user interface, application logic, and database operations to be maintained independently.

D. Validation

Input validation is used to prevent incomplete or invalid submissions, including phone-number format validation, required-field validation, URL validation, report-form validation, and validation of uploaded

information, along with file/upload restrictions where applicable. Validation helps reduce incorrect or incomplete data from being processed.

E. Risk Analysis

The application performs rule-based risk analysis on the available information and presents a risk score together with warning signs, explanations, and recommended actions. The risk score is intended as a decision-support feature and does not represent a legal determination that a message, URL, phone number, or person is fraudulent.

V. RESULTS AND DISCUSSION

A. Prototype Results

The developed Digital Safety Assistant successfully demonstrates the main functions proposed by the research. The Home module provides simple navigation to the main safety functions, and the Check Something functionality supports suspicious message, screenshot, phone-number, and URL analysis, presenting risk-related information in an understandable form. The application also provides fraud reporting, awareness and learning material, an interactive quiz, language support, Easy Mode, voice assistance/input, evidence guidance, trusted-person support, and official safety resources. The backend was implemented using Java and Spring Boot, the frontend uses HTML, CSS, and JavaScript, and MySQL is used as the relational database with Spring Data JPA providing database access. The application can be run as a Spring Boot web application during development and testing.

B. Discussion

The developed system demonstrates the feasibility of combining cybersecurity education with practical risk-analysis and fraud-assistance functionality in a single beginner-friendly web application. Instead of requiring users to understand technical cybersecurity terminology, the application presents risk information through scores, warning signs, explanations, and recommended actions. The inclusion of message, screenshot, phone-number, and URL analysis provides users with multiple ways to examine suspicious situations, while awareness material and the interactive quiz complement the analysis features by helping users learn safer cybersecurity practices. The Java Spring Boot and MySQL architecture provides a structured foundation for future expansion, and the separation of controllers, services, repositories, and entities supports maintainability.

However, the technical success of the application does not by itself demonstrate an improvement in users' cybersecurity awareness. A structured user evaluation using pre-test and post-test measurements, as described in Section III-F, is therefore required before making claims about awareness improvement.

C. Current Limitations

1. Risk analysis is based on programmed rules and available information and should not be treated as a guaranteed fraud-detection mechanism.
2. A low-risk result does not guarantee that a message, URL, phone number, or website is safe.
3. User-generated fraud reports require appropriate verification and moderation.
4. The application does not automatically determine legal fraud or criminal responsibility.
5. Automatic monitoring of incoming calls and call logs is not implemented.
6. The accuracy of risk analysis can be improved by using larger and properly validated datasets.
7. A formal user-awareness study has not yet been completed.
8. The awareness content can be expanded with additional real-world fraud scenarios.

VI. CONCLUSION AND FUTURE SCOPE

Cybersecurity awareness is increasingly important as people depend on smartphones, digital payments, online banking, and internet-based services. Users with limited digital literacy may face difficulties in identifying fraudulent communication and following appropriate cybersecurity practices. This research proposed and developed a simple cybersecurity-awareness and fraud-assistance web application designed around the needs of digitally less-literate users. The system integrates suspicious message, screenshot, phone-number, and URL checking with risk analysis, warning signs, explanations, and recommended actions, alongside fraud reporting, cybersecurity awareness content, an interactive quiz, language support, Easy Mode, voice assistance, trusted-person support, evidence guidance, and official safety resources.

The application was developed using Java, Spring Boot, Spring Web, Spring Data JPA, Maven, HTML, CSS, JavaScript, and MySQL. The layered backend architecture using controllers, services, repositories, and entities provides a structured foundation for further development. Technical testing demonstrated that the application can be built and executed as a Spring Boot web application and that the major application components are functioning. However, technical functionality alone cannot establish whether the application improves cybersecurity awareness; a user-based evaluation using pre-test and post-test measurements is required before making claims about awareness improvement.

Future development can include:

1. Expansion of the MySQL database with properly sourced and verified fraud information.
2. Improved report moderation and verification mechanisms.
3. Larger and more comprehensive datasets for risk analysis.
4. Improved rule-based risk analysis for messages, screenshots, phone numbers, and URLs.
5. Machine-learning-based risk analysis after collecting an appropriate and ethically managed dataset.
6. Additional regional-language support and improved voice-based assistance for users with reading difficulties.
7. Improved accessibility using larger text, simple icons, and clearer instructions.
8. Pre-test/post-test user evaluation with the intended population, and longer-term evaluation to study whether cybersecurity awareness is retained.
9. Community-based alerts for appropriately verified threats and improved trusted-person and assistance features.
10. Analytics to understand which awareness topics users find most useful.
11. Responsible research into caller-identification capabilities while following applicable privacy, permission, and platform requirements.
12. Integration with additional official cybersecurity resources and reporting mechanisms.

The research provides a foundation for developing a practical cybersecurity-awareness tool that combines education, risk analysis, and user-oriented fraud assistance in a single accessible web application.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my research guide for providing valuable guidance, suggestions, and support throughout this research work. I also thank the faculty members and my institution for providing the academic resources and environment required for completing the study. I am grateful to everyone who contributed suggestions and feedback during the development and testing of the application.

REFERENCES

[1] C. Pascoe, S. Quinn, and K. Scarfone, “The NIST Cybersecurity Framework (CSF) 2.0,” *NIST Cybersecurity White Paper (CSWP 29)*, National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29.

[2] F. J. Rocha Estrada, C. E. George-Reyes, and L. D. Glasserman-Morales, “Security as an emerging dimension of Digital Literacy for education: A systematic literature review,” Journal of e-Learning and Knowledge Society, 2022, doi: 10.20368/1971-8829/1135440.

[3] “A systematic review on digital literacy,” BMC / PubMed Central, 2022.

[4] N. A. G. Arachchilage and S. Love, “Security awareness of computer users: A phishing threat avoidance perspective,” Computers in Human Behavior, vol. 38, pp. 304–312, 2014, doi: 10.1016/j.chb.2014.05.046.

[5] J. Prümmer, T. van Steen, and B. van den Berg, “A systematic review of current cybersecurity training methods,” Computers & Security, vol. 136, Art. no. 103585, 2024, doi: 10.1016/j.cose.2023.103585.

[6] “Assessing the effect of cybersecurity training on End-users: A Meta-analysis,” Computers & Security, Art. no. 104206, 2024, doi: 10.1016/j.cose.2024.104206.

[7] N. H. A. Rahim, S. Hamid, K. M. L. Mat, S. Shamshirband, and S. Furnell, “A systematic review of approaches to assessing cybersecurity awareness,” Kybernetes, vol. 44, no. 4, pp. 606–622, 2015.

[8] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, “Information security awareness and behavior: A theory-based literature review,”

Management Research Review, vol. 37, no. 12, pp. 1049–1092, 2014, doi: 10.1108/MRR-04-2013-0085.

[9] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," Heliyon, vol. 9, no. 3, Art. no. e14234, 2023, doi: 10.1016/j.heliyon. 2023.e14234.

[10] N. A. G. Arachchilage and S. Love, "A game design framework for avoiding phishing attacks," Computers in Human Behavior, vol. 29, no. 3, pp. 706–714, 2013, doi: 10.1016/j.chb.2012.12.018.

[11] N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," Computers in Human Behavior, vol. 60, pp. 185–197, 2016, doi: 10.1016/j.chb.2016.02.065.

[12] M. H. R. Atta et al., "Safeguarding seniors in the digital age: An experimental study on the influence of cybersecurity awareness training on technology adoption, security behaviors, and cybercrime consciousness," Frontiers in Public Health, 2026, doi: 10.3389/fpubh.2026.1780758.

[13] S. Kazamia, C. Culnane, D. Gardham, S. Prior, and H. Treharne, "Phish and Tips: Phishing Awareness and Education for Older Adults," in Human Aspects of Information Security and Assurance, 2024.

[14] K. Khando, S. Gao, M. S. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," Computers & Security, vol. 106, Art. no. 102267, 2021, doi: 10.1016/j.cose.2021.102267.

[15] T. Fertig and A. E. Schütz, "About the measuring of information security awareness: A systematic literature review," in Proc. 53rd Hawaii Int. Conf. System Sciences, 2020, doi: 10.24251/HICSS.2020.798.

[16] "Driving behaviour change with cybersecurity awareness," *Computers & Security*, vol. 142, Art. no. 103858, 2024.