Journal of Information Systems and Informatics
Vol. 7, No. 1, March 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i1.1034 Published By DRPM-UBD

Innovating Cybersecurity in Tanzanian Academia: A Mobile Tool for Combatting Social Engineering Threats

Lucas Hosea Mjema[1], Bonny Said Mgawe[1], Mussa Ally Dida[1]

[1] School of Computational and Communication Science and Engineering, The Nelson Mandela African Institution of Science and Technology
Email: [1]mjemal@nm-aist.ac.tz, [1]bonny.mgawe@nm-aist.ac.tz, [1]mussa.ally@nm-aist.ac.tz

Abstract

Social engineering attacks, including phishing, smishing, and vishing, pose significant threats to higher learning institutions, especially in regions with limited cybersecurity awareness and weak incident reporting mechanisms. This study introduces a novel mobile tool that combines real-time threat detection, streamlined reporting, and personalized training to address these vulnerabilities. Using a mixed-methods approach, we gathered survey data from 395 participants, conducted interviews with 10 IT professionals, and ran a pilot test with 20 users. The proposed tool provides instant scanning of emails/SMS for social engineering content and instant incident reporting alongside interactive, bilingual (English/Swahili) training modules. Results show a substantial improvement in user awareness, 85% of users reported a better understanding of social engineering threats after using the app, and high user satisfaction, with 90% expressing approval of the intuitive interface. The integration of real-time threat analysis and immediate reporting with tailored education distinguishes our tool from existing solutions. We discuss how bilingual support broadened engagement and how personalized learning paths reinforced retention of security best practices. Our findings demonstrate that a mobile-based, user-centric approach can significantly bolster cybersecurity awareness and incident response in academic environments. Future work will integrate machine learning for enhanced threat detection and voice-guided features for accessibility, aiming to continuously adapt to evolving attack strategies. This research provides insights for policymakers on incorporating such tools into broader institutional cybersecurity strategies.

Keywords: Social Engineering Awareness, Mobile-Based Application, User-Centric Tool, Vulnerabilities, Phishing, Smishing, Cybersecurity Training, Incident Response

1. INTRODUCTION

Social engineering is one of the most pervasive cybersecurity threats, and educational institutions have become prime targets [1]. Attackers exploit human factors through tactics like phishing (deceptive emails), smishing (malicious SMS), and vishing (voice scams) to trick users into divulging sensitive information or compromising systems [2]. Studies have consistently highlighted that user susceptibility, influenced significantly by individual behavior and cognitive factors, remains a critical vulnerability in cybersecurity defenses [3], [4]. The education sector's decentralized IT systems and diverse user base make it particularly vulnerable [5][6]. In Tanzania and similar underdeveloped regions, many universities lack adequate cybersecurity awareness programs and efficient incident reporting channels [6] [7]. Recent studies and incident reports underscore the urgency: for example, more than half of surveyed universities in one study experienced cyber-attacks on a weekly basis, with 61% suffering data loss or financial damage as a result [5].

Similarly, Al-Janabi and Al-Shourbaji [8] reported notably low levels of cybersecurity awareness in educational environments across the Middle East, further emphasizing the global relevance and urgency of addressing cybersecurity education gaps. At a regional level, analyses have highlighted ongoing challenges – *e.g.*, a 2015 assessment noted systemic weaknesses in East African educational cybersecurity practices [9], and a 2019 case study of two Tanzanian universities revealed numerous security threats and vulnerabilities in campus networks [6]. Even in 2022, information security in Tanzanian higher learning institutions was described as "a disaster," largely due to insufficient awareness and training [10]. The rapid shift to online learning and increased Internet connectivity during the COVID-19 pandemic further expanded the attack surface, exposing African universities to greater cybercrime risks [7]. Surveys in Sudan, for instance, found that most undergraduate students have low cybersecurity awareness [7], illustrating a widespread need for improved cybersecurity education in academia.

Effective countermeasures require not only technical defences but also addressing the human element, as users are often the weakest link [11][12]. Low awareness and unsafe practices among students and staff can undermine security even when technical controls are in place [10]. Experts emphasize that cultivating a strong security culture through continuous awareness and training is critical [13]. Unfortunately, traditional one-off seminars or static training sessions have proven insufficient to produce lasting behavioural change [14]. Many conventional programs fail to engage users or keep up with evolving social engineering tactics [14][1]. Security awareness campaigns need to be ongoing and adaptive, not one-time events, to effectively change behaviour [14]. Prior work has shown that when training is generic or infrequent, users may quickly revert to unsafe habits, especially under operational pressures and convenience trade-offs [15]. Moreover, language and contextual barriers can impede understanding; in Tanzania, where English may not be every user's first language, delivering content in a familiar language (Swahili) can greatly improve comprehension and engagement.

A number of studies have explored strategies to raise cybersecurity awareness in organizations. Some have proposed comprehensive frameworks or educational curricula for higher education [16], while others have focused on particular demographics (such as college students or faculty) and found significant gaps in awareness that need to be addressed [7][10]. It is widely accepted that user-centric and practical training approaches yield better outcomes than purely theoretical ones [12][17].

In particular, personalized training, tailoring content to an individual's role and behaviour, has been identified as more effective at instilling good security practices than "one-size-fits-all" methods [17]. Likewise, interactive tools (such as quizzes or games) tend to engage users more than passive videos or lectures [18]. Havenstein [19] further confirms that gamified training significantly improves engagement and retention of cybersecurity principles compared to conventional training approaches. However, despite these insights, there remains a lack of scalable solutions in the context of higher education that combine awareness training with actionable incident response. Many universities still rely on outdated or ad-hoc incident reporting (e.g. forwarding phishing emails to an IT helpdesk) [20], which often leads to delayed or under-reported security incidents.

To address these gaps, we developed a mobile-based tool specifically designed for higher learning institutions in Tanzania. We chose a mobile application platform given the ubiquity of smartphones among students and staff, which ensures accessibility and encourages frequent interaction. This approach is particularly timely given the increased reliance on mobile technologies for cybersecurity education during and after the COVID-19 pandemic, as highlighted by Yin et al. [21]. Notably, research suggests that users' cybersecurity practices on mobile devices often lag behind, smartphones can be a "victim of operational pressures" where convenience outweighs caution [15]. This reinforces the importance of delivering awareness content directly on mobile devices. Our tool integrates interactive learning modules with real-time threat detection and reporting capabilities. Unlike traditional programs that might, for example, offer a quiz or a handbook, our solution actively engages users by allowing them to scan emails or SMS messages for phishing indicators on the fly and report suspicious content with a single tap. The application provides immediate feedback, if a user scans a message, the tool uses built-in rules of thumb to inform them whether it's potentially malicious, educating the user in the moment of decision. This instant feedback loop helps users learn to recognize threats in their daily communications, reinforcing training through practice.

Key features of the tool include: (1) Personalized assessments: the app has a section for quizzes where users can assess their knowledge on social engineering scenarios and adapts the difficulty based on their performance, focusing on areas where a particular user shows weaker understanding; (2) Bilingual support: all content (tutorials, quizzes, alerts) is available in both English and Swahili, to ensure language is not a barrier to understanding technical security concepts; (3) Instant threat analysis: users can tap a switch to enable auto scanning of email or SMS via an email/SMS API to check for phishing and smishing red flags (suspicious links, senders, etc.) and returns an immediate risk assessment; and (4) One-touch incident reporting: if a message is deemed suspicious, the user can report it through the app, which automatically forwards relevant details to institutional cybersecurity personnel for further investigation. By combining training and incident reporting in a single platform, the tool not only educates users but also actively involves them in the institution's security process. This approach creates a feedback synergy: as users report incidents, the IT security team can respond faster to real threats [20], and the user receives confirmation and additional guidance, which reinforces their learning. Comparison between the proposed mobile tool and existing solutions can be seen in Table 1.

Table 1. Summary of the proposed mobile-based app features

	System	IIR	MB	UAT	IA	GR	TA
1	Smith et al. (Web-based solution)	x	x	✓	✓	x	x
2	Havenstein (Game-based solution)	x	x	✓	x	x	x
3	Wang et al. (AI-driven corporate model)	x	x	✓	x	x	x
4	Proposed Mobile-Based Application	✓	✓	✓	✓	✓	✓

Key: IIR – Instant Incident Reporting, MB – Mobile-Based, UAT – User Awareness Training, IA – Interactive Assessments, GR – Generate Report, TA – Threat Analysis (Email & SMS API)

This work presents an innovative, complete approach to strengthening human factors in cybersecurity within academia. It extends the literature by demonstrating how a mobile, user-focused application can simultaneously raise awareness and improve incident handling. To our knowledge, this is the first mobile-based tool developed specifically for Tanzanian academic contexts that integrates real-time threat detection, bilingual interactive assessments, and seamless incident reporting. The following sections detail our methodology (including how qualitative insights shaped the tool's design), the features of the developed application, and an evaluation of its effectiveness through pilot deployment. We also discuss the implications of bilingual and personalized features on user engagement, and how similar tools could benefit other educational institutions in developing countries.

Our conclusion outlines future directions, including the integration of machine learning for even more robust real-time threat detection, and how the outcomes of this study can inform broader cybersecurity policies for the education sector.

2. MATERIALS AND METHODS

The research workflow followed a structured four-stage approach, depicted in Figure 1, which guided our methodology clearly from requirements collection through final deployment.

2.1 Research Design and Workflow

This study adopted a mixed-methods approach comprising surveys, interviews, and iterative prototyping. The overall research and development process followed a structured workflow, as illustrated in Figure 1. Figure 1 outlines each stage: requirements gathering, tool development, feedback integration, and deployment. We first conducted a requirements analysis (Stage 1 in Figure 1) to ground the project in actual institutional needs. This involved a survey of end-users and interviews with experts to identify prevalent social engineering vulnerabilities and user requirements. Based on these insights, we defined the system requirements and design objectives for the mobile tool. Next, we proceeded with Agile development (Stage 2), implementing features in iterative sprints. After initial development, we carried out a pilot deployment (Stage 3) for user testing and gathered qualitative feedback on usability and effectiveness. Finally, we refined the tool (Stage 4) and evaluated its impact on user awareness and reporting behaviour. Each component of Figure 1 corresponds to a specific phase of our methodology, which we explain as follows.

1) Requirements Gathering

We began by collecting data on the current state of social engineering awareness and incident response in the target institutions. We distributed an online survey to students, academic staff, and administrative staff across several Tanzanian universities. A total of 395 responses were collected, exceeding our target sample size (we initially aimed for ~385 based on sample size estimation for the population). The survey included both quantitative questions (e.g. asking participants to rate their knowledge of phishing or whether they had fallen victim to attacks) and qualitative prompts (e.g. asking for descriptions of any suspicious emails or messages they had encountered). In parallel, we conducted semi-structured interviews with 10 IT professionals and cybersecurity experts from the higher education sector. These experts, each with experience managing campus IT security, provided deeper insight into institutional challenges – for example, common attack patterns they observed and difficulties in the existing incident reporting workflows. We continued interviews until we reached a point of data saturation, where no new themes were emerging. The qualitative findings were invaluable: recurring themes included the lack of an easy-to-use reporting mechanism for phishing attempts, and the observation that many users were unaware of subtler social engineering ploys beyond basic phishing. We carefully documented these needs. For instance, experts highlighted that non-technical staff often ignored suspicious SMS messages due to uncertainty, indicating a need for an SMS scanning feature. These insights directly influenced the features of our tool, we translated the needs into specific functional requirements. Table 2 summarizes some of these requirements, such as *"the system shall provide a one-click way to report phishing attempts"* or *"the system shall offer content in Swahili for non-English-preferring users."* By grounding requirements in real user feedback, we ensured the tool's design was problem-driven and user-centric. Notably, features like the bilingual interface and simplified incident reporting were implemented specifically because the interviewees and survey respondents indicated those as priorities.

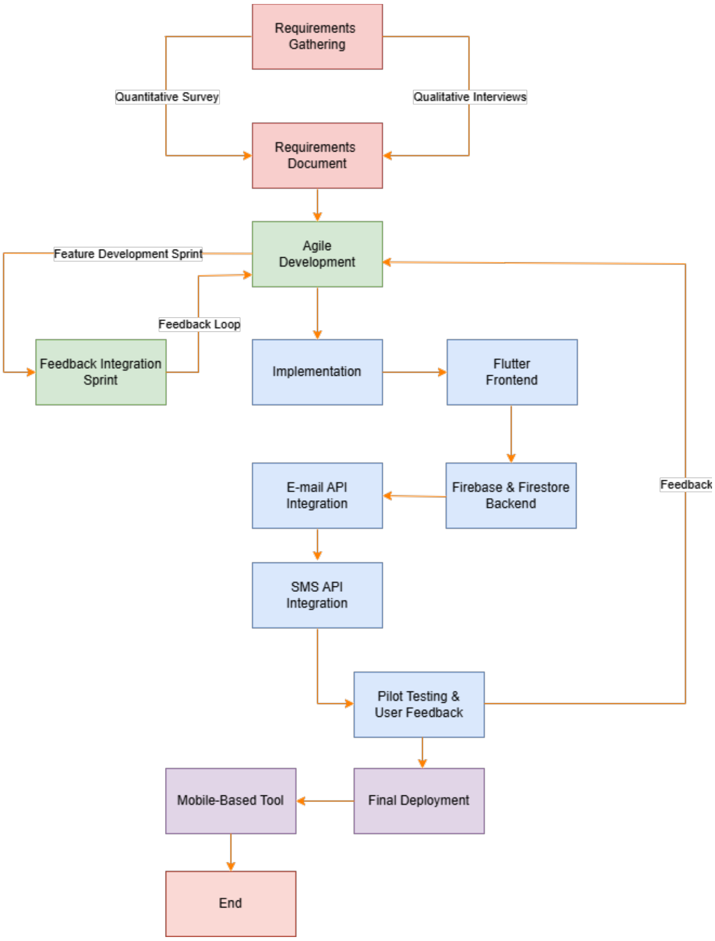


Figure 1. Research Design and Workflow for Mobile-Based Tool

Table 2. Functional Requirements

	Feature	Description	User Role
1	Login and Registration Screen	Users register using institutional email and password, with options for language selection (English or Swahili).	All Users
2	Getting Started Screen Module	Introduces users to social engineering and its types (phishing, smishing, vishing, pretexting, baiting).	All Users
3	Assessment Screen Module	Provides interactive assessments on social engineering threats, with instant feedback and score tracking.	All Users
4	View Reports Screen Module	Allows admins to view summary reports of user assessments and download detailed PDF reports.	Admin Only
5	Training Modules Screen	Provides users with access to general training modules for improving their understanding of social engineering threats.	All Users
6	Add Quiz Screen Module	Enables admins to create new assessments by adding individual questions or uploading predefined templates for bulk entry.	Admin Only
7	Add Training Resources	Allows admins to upload training resources related to different social engineering categories for users to access.	Admin Only
8	Social Engineering (SE) Analysis Screen Module	Users can scan emails and SMS for potential social engineering threats using threat detection algorithms.	All Users

2) Agile Development

Guided by the gathered requirements, we proceeded to develop the mobile application following Agile principles. The development phase was organized into iterative sprints (each approximately two weeks long). In each sprint, we implemented a set of features and then performed internal testing. The core technology stack included Flutter for cross-platform mobile development (ensuring the app runs on Android devices prevalent among students) and Firebase for the backend services. Early development sprints focused on building the foundational features: user authentication (restricted to institutional email domains for security), the training module framework, and the incident reporting module. Subsequent sprints integrated the more advanced capabilities such as the email/SMS analysis API. For this, we utilized an Email scanning API and an SMS parsing library to analyse message content for known phishing indicators (e.g., comparing URLs against a blacklist, checking sender addresses). Throughout development, we maintained close alignment with user needs as identified earlier. For example, when implementing the user interface, we kept it as simple as possible, the survey had revealed that a significant portion of users were not highly tech-savvy. In response, we ensured the home screen provided straightforward navigation with large icons (e.g., "Social Engineering (SE) Analysis," "Start Assessment," "Report an Incident") and minimal text. We also incorporated visual cues and local language labels in the interface, reflecting feedback that technical jargon was a barrier for some users. The development process was iterative: after each major feature addition, we performed a quick round of informal testing with a few volunteer users (outside the main pilot group) to gather immediate impressions and catch obvious usability issues.

3) Pilot Testing and Feedback Integration

After the core features were implemented, we conducted a pilot test with 20 participants from the target user community (including students and staff). This pilot served as both a usability test and a preliminary evaluation of effectiveness. The selection of 20 participants was informed by widely accepted practices in usability and pilot studies, where small but representative samples typically provide sufficient insights to identify usability issues and refine the application effectively. According to Alroobaea and Mayhew [22], pilot tests involving approximately 15 to 20 users are generally adequate to uncover most usability problems in technology-based tools. Furthermore, existing literature on usability studies within educational technology contexts often endorses sample sizes ranging between 10 and 30 participants as effective for capturing detailed, actionable user feedback without overwhelming resources. Each pilot user installed the app on their own smartphone and used it for a period of two weeks. We provided them with a brief orientation on the app's functions, then allowed them to use it naturally as they encountered emails or texts, and also encouraged them to explore the training quizzes. During this phase, we collected feedback via a user acceptance survey and follow-up interviews with pilot users. We specifically asked pilot users about any difficulties they encountered, features they liked or did not use, and suggestions for improvement. This qualitative feedback was then analysed and fed back into a final development sprint to refine the tool. For example, pilot users indicated that switching between English and Swahili content in the app could be smoother, so we added a persistent language toggle on each screen. Some users requested more examples in the training module, in response, we expanded the question bank of phishing examples (including locally relevant examples, such as fake scholarship offer scams that had been reported in the community). We also adjusted the alert messages from the email/SMS scanner to be more user-friendly; earlier pilot feedback noted that a few alerts were too technical, so we rephrased them in simple terms (e.g., “This link looks suspicious, be careful!” instead of a complex description of why it was flagged).

4) Deployment and Data Collection

The finalized version of the mobile-based application was deployed to selected participants drawn from the initial survey group of 395 respondents. Participants received clear instructions on downloading, installing, and using the app. They were guided on how to navigate core features, such as interactive assessments, incident reporting, and real-time email and SMS threat analysis. Participants were encouraged to integrate the tool naturally into their daily interactions with potentially suspicious communications to ensure realistic usage. During this phase, we ensured adherence to ethical guidelines by securing informed consent from all participants and anonymizing all data collected through the application. Technical support was provided to participants throughout the deployment phase, addressing any operational or usability concerns promptly to ensure continuous and consistent user engagement. Data from user interactions with the app were securely stored via the Firebase backend, ensuring efficient data synchronization and management.

2.2. Participants and Data Collection Instruments

1) Survey

The initial survey captured demographic information, baseline awareness levels, and prior exposure to social engineering. Participants ranged from undergraduate students to senior faculty. Table 3 (in Results) summarizes key demographic statistics. The survey included knowledge questions (e.g., “How would you rate your knowledge of phishing attacks?” with options from *No knowledge* to *Expert knowledge*) and behavioural questions (e.g., “Have you ever clicked a suspicious link or responded to a dubious message?”). It also inquired whether participants had attended any cybersecurity training before, to gauge prior exposure. After using the tool, participants were given a follow-up survey repeating some knowledge questions and asking about their experience with the app (usefulness, ease of use, etc.).

2) Interviews

We used a semi-structured interview guide for the expert interviews and pilot user interviews. For experts, questions focused on current institutional practices (like “How are phishing incidents currently reported and handled?”) and perceptions of user weaknesses (“What security mistakes do you observe frequently among students or staff?”). For pilot users, questions were more about their interaction with the app ("Which feature did you find most helpful or interesting?" and "Did the app make you feel more confident about recognizing scams?").

3) Data Analysis

Quantitative survey data were analysed with SPSS v27. We performed descriptive statistics and paired t-tests on pre- and post-intervention responses to assess improvement in awareness (e.g., whether the self-reported knowledge levels increased significantly). Qualitative data (interview transcripts and open-ended survey comments) were analysed using thematic coding. We identified recurring themes such as *improved vigilance*, *interface usability*, *language accessibility*, and *reporting confidence* from the participant feedback. These qualitative themes are used in the discussion to explain and add context to the numeric results. The next section presents the results of the survey and interview findings together, structured by theme, and discusses them with reference to the research objectives and related work.

3. RESULTS AND DISCUSSION

3.1. Demographics of Participants

The study involved 395 participants from various higher learning institutions in Tanzania. Students represented the largest group (60%), followed by academic staff (30.1%) and administrative staff (9.9%). Participants were predominantly aged between 18 and 35 years (74.4%), with the remaining participants over 35. Gender distribution included 69.6% male and 30.4% female respondents, as summarized in Table 3.

Table 3. Demographic of Participants

Variable	Category	Frequency	Percentage
Gender	Female	275	69.6
	Male	120	30.4
	Total	**395**	**100**
Role at the Institution	Academic Staff	119	30.1
	Administrative Staff	39	9.9
	Student/Scholar	237	60.0
	Total	**395**	**100**
Age of Respondents (years)	18 – 25	153	38.7
	26 – 35	141	35.7
	36 – 45	83	21.0
	Above 46	18	4.6
	Total	**395**	**100**

3.2. Awareness of Social Engineering Attacks and Cybersecurity Training

Most respondents (74%) indicated awareness of social engineering threats. However, their knowledge varied, with 47% reporting basic knowledge, 34% good knowledge, and only 9% considered themselves experts. Additionally, only 38% had participated in formal cybersecurity training, underscoring a significant gap in comprehensive education initiatives within these institutions (Figure 2).

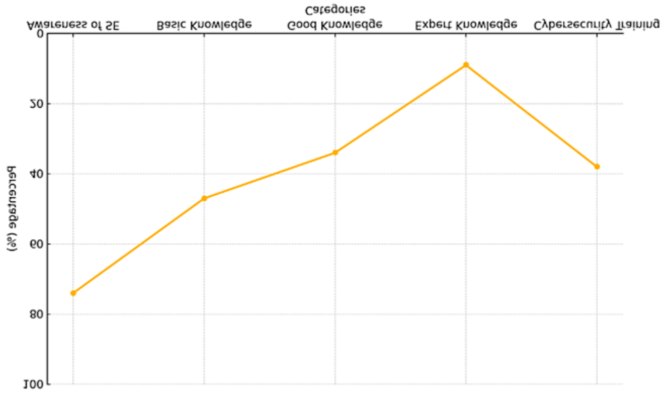


Figure 2. Social Engineering Awareness and Attending Cybersecurity Training

3.3 Experience with Social Engineering Attacks

Of the total respondents, 45% reported experiencing social engineering attacks, predominantly phishing (28%) and smishing (15%). Academic and administrative staff, frequently managing sensitive information, reported the highest incidence of such attacks. These incidents commonly involved fraudulent emails or SMS messages aiming to collect sensitive personal or financial information (Figure 3).

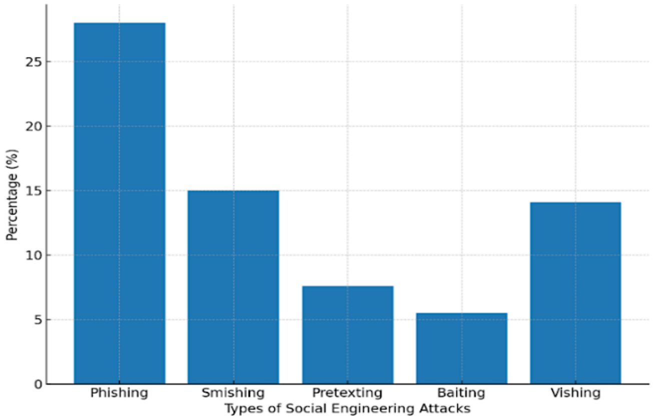


Figure 3. Respondents Experience with Social Engineering Attacks

3.4. Reporting and Behavioral Pattern

While 59% of respondents had either experienced or knew someone who had experienced a social engineering attack, only 32% reported such incidents to institutional authorities. Primary reasons for not reporting included unclear reporting mechanisms and low confidence in the institutional response. Additionally, 23% expressed dissatisfaction with the handling of reported incidents, highlighting a communication gap between users and cybersecurity teams (Figure 4).

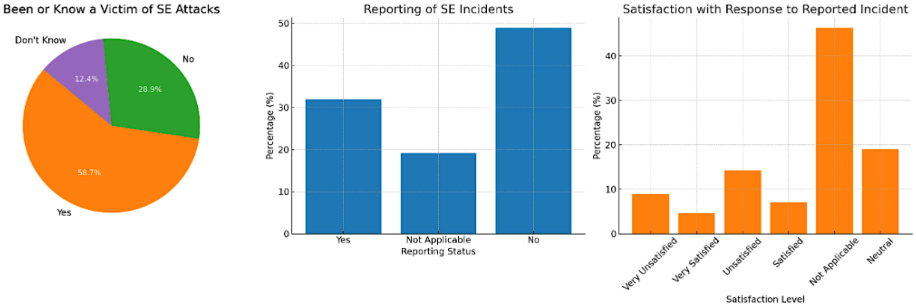


Figure 4. Reporting and Behavioral Patterns

3.5. Perceived Effectiveness and Willingness to Use a Mobile-Based Application

Respondents expressed positive attitudes toward the proposed mobile-based tool. Of all participants, 64% perceived the application as either effective or very effective for improving social engineering awareness and incident reporting within institutions. Moreover, 85% indicated willingness to use the application to enhance their cybersecurity knowledge and protection capabilities, reflecting strong potential for adoption and effectiveness (Figure 5).

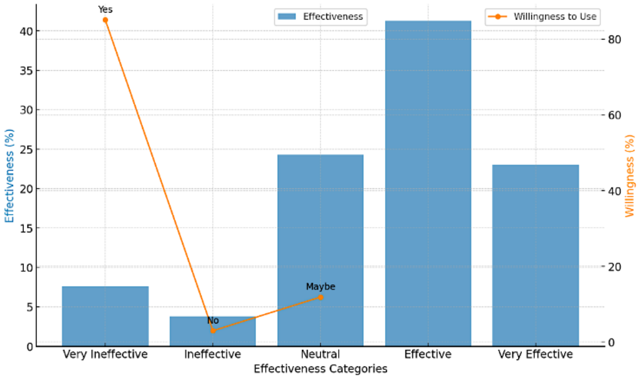


Figure 5. Effectiveness and Willingness to Use a Mobile-Based Application

3.6. Interview Results

Structured interviews with ten IT professionals and cybersecurity experts revealed three critical themes regarding institutional cybersecurity challenges:

1) Lack of effective incident reporting mechanisms: Experts highlighted delayed responses due to unclear or inaccessible reporting systems.
2) Need for user-friendly tools: Existing tools lacked interactivity and engagement necessary for effective cybersecurity training.
3) Resource constraints: Budget and technological limitations significantly hindered institutions from implementing advanced cybersecurity measures, as summarized in Table 4.

Table 4. User Stories

ID	Role	User Stories	Key Theme
1.	IT Security Officer(s)	“As an IT Security Officer, I often don't receive timely reports on security incidents due to a lack of clear, accessible reporting mechanisms. This delays our ability to respond effectively to potential social engineering threats.”	Lack of Incident Reporting Mechanisms
2.	ICT officer(s)	“As an IT Officer, I need a simple, user-friendly tool to educate staff and students on social engineering attacks, but the currently there are no tools that conducts assessments and training or engaging to users.”	Need for User-Friendly Tools
3.	Head, ICT Department(s)	“As a head of ICT department, I face significant challenges in implementing advanced cybersecurity solutions due to budget and resource constraints (Technology). This leaves our institution vulnerable to social engineering attacks.”	Resource Limitations

These insights directly influenced the final design and functionality of the mobile-based application, emphasizing streamlined incident reporting, interactive and engaging training modules, and cost-effective implementation through scalable technology.

3.7. System Development Results

3.7.1. System Design

The proposed mobile-based tool was developed using the Flutter framework for the frontend, ensuring a responsive and user-friendly interface across multiple device types. Firebase was employed for backend services, providing instant data synchronization and user authentication, while Firestore was used to manage data related to user profiles, assessments, and incident reports as illustrated in Figure 6. The tool integrates both an Email API and an SMS API to allow for instant scanning of emails and SMS messages for potential social engineering threats, such as phishing and smishing. This functionality enables users to report suspicious communications directly from their mobile devices. The development process followed the Agile methodology, allowing for iterative refinement of features based on continuous feedback gathered from users during the pilot testing phase. This ensured that the tool was not only functional but also adaptable to the specific needs of higher learning institutions.

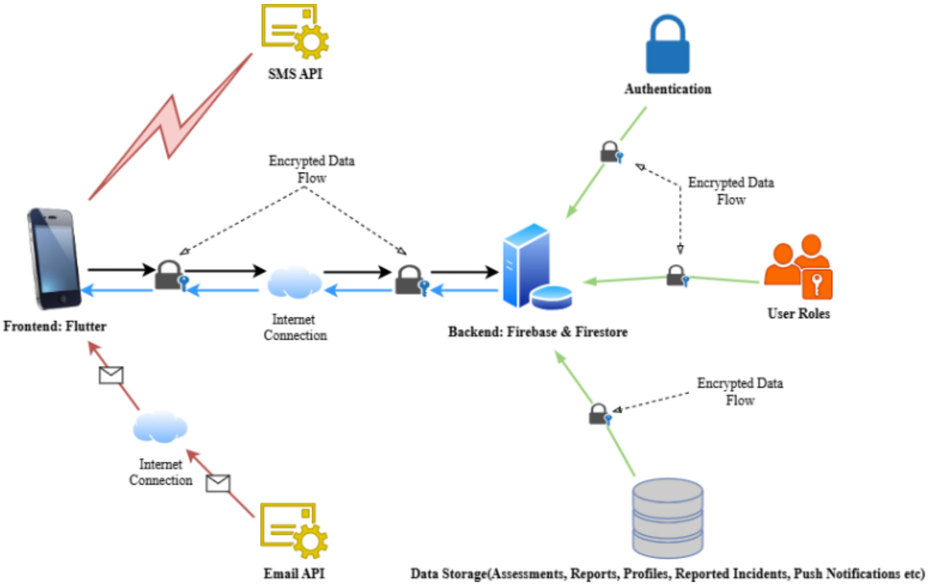


Figure 6. Conceptual Diagram

3.7.2. Use case Diagram

Figure 7 presents the use case diagram, highlighting interactions between different user roles and the mobile application's functionalities identified from qualitative user requirements.

3.7.3 Backend Architecture

The backend architecture for the mobile-based application is built on Firebase and Firestore, providing user authentication, data storage, instant notifications, and incident reporting capabilities (Figure 8). The system uses Firebase Authentication to manage user registration and login, allowing users to securely create accounts using their institutional domain email and password. This ensures that only authorized users can access the tool's features. All data is stored in Firestore, a NoSQL cloud database. Several collections are created to organize different types of information, such as user profiles and roles, assessment results, quiz questions, training modules, reported incidents, and acknowledgements for reported incidents. This structured data storage allows the app to handle large amounts of data in a scalable and organized way.

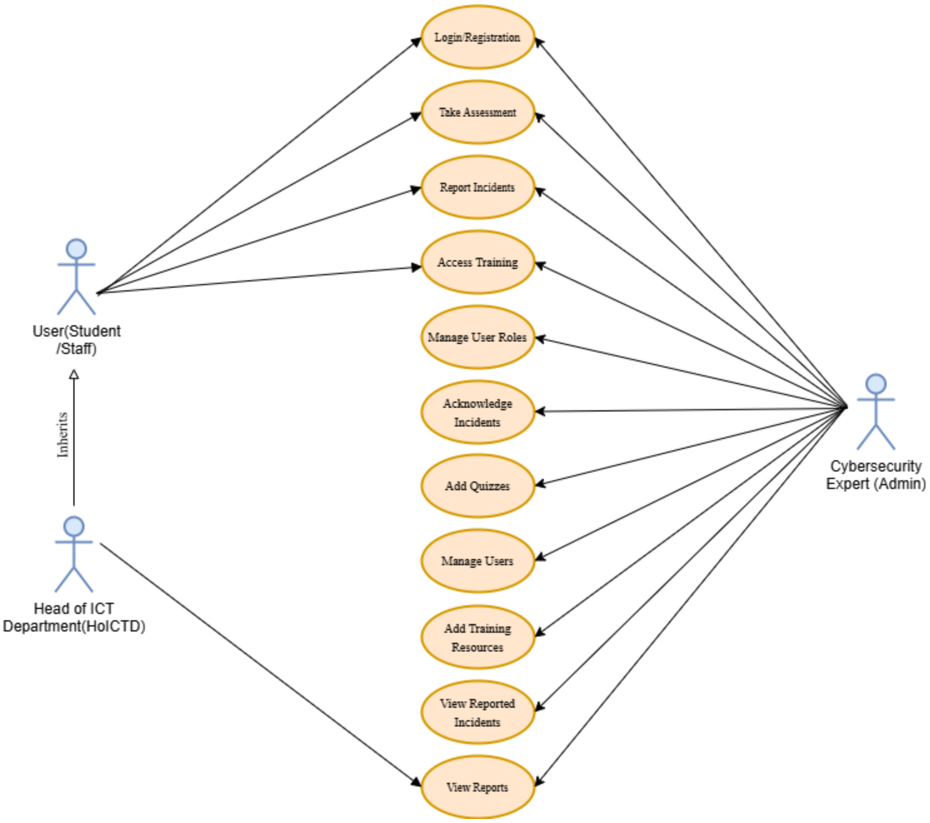


Figure 7. Use case Diagram

Firestore's instant data synchronization enables dynamic updates, ensuring that changes made in the app, such as a user submitting a reported incident, are immediately reflected in the backend. This feature is crucial for the incident reporting system, which logs suspicious email and SMS incidents reported by users. The app's backend also includes a polling mechanism that periodically checks the Firestore database for new incidents. When a new report is detected, the app triggers a local notification, alerting the admin instantly. This system improves response times by notifying the admin as soon as new incidents are reported.

To optimize data retrieval, Firestore indexes are used in the assessments and reported incidents modules. These indexes improve query performance and ensure that even as the dataset grows, data retrieval remains efficient. This is particularly important for the admin's report view, where large datasets are often accessed. The mobile app is connected to Firebase through the API provided by Firebase, along with the necessary SHA certificate fingerprints. Additionally, the Firebase SDK and the Google Services JSON file are integrated into the Flutter codebase, allowing seamless communication between the mobile app and the Firebase backend. These components ensure that the app's authentication, data storage, and notification systems function properly, providing a smooth user experience.

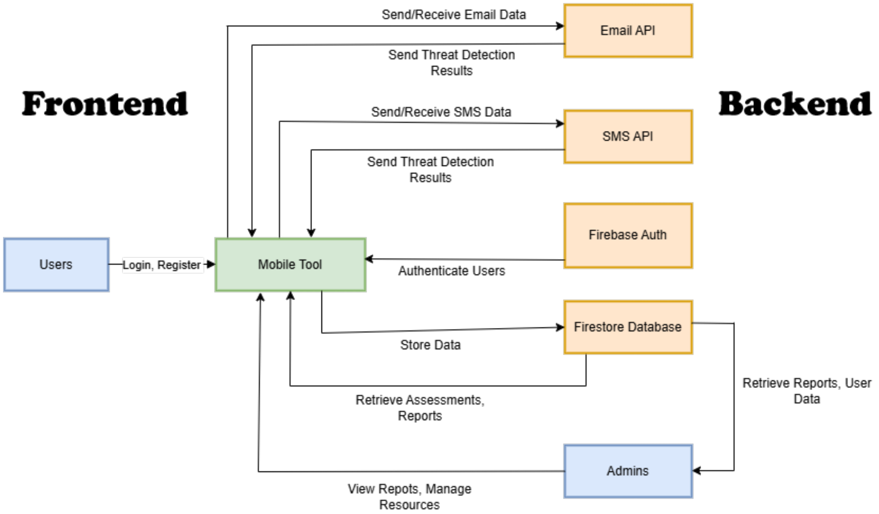


Figure 8. Frontend and Backend Interactions

3.8. Designed Interfaces

The mobile-based application features a variety of user interfaces designed to provide a seamless and intuitive experience for users across different roles. The following sections describe the core screens that make up the main functionalities of the tool. While these are the primary interfaces, additional screens exist to support various administrative and user-specific actions within the app.

3.8.1. Login/Registration and Dashboard Screen

The Login/Registration Screen allows users to register with their institutional email and password or log in if they already have an account. Upon successful login, users are directed to the Dashboard, which serves as the central hub for accessing all core features of the app (Figure 9). The dashboard displays options for starting assessments, reporting incidents, viewing training modules, and accessing the user profile. It also includes navigation options for administrators, such as managing quizzes, viewing reported incidents, and accessing training materials. The interface is designed to be intuitive, with clear icons and labels to make navigation easy for users across all roles.

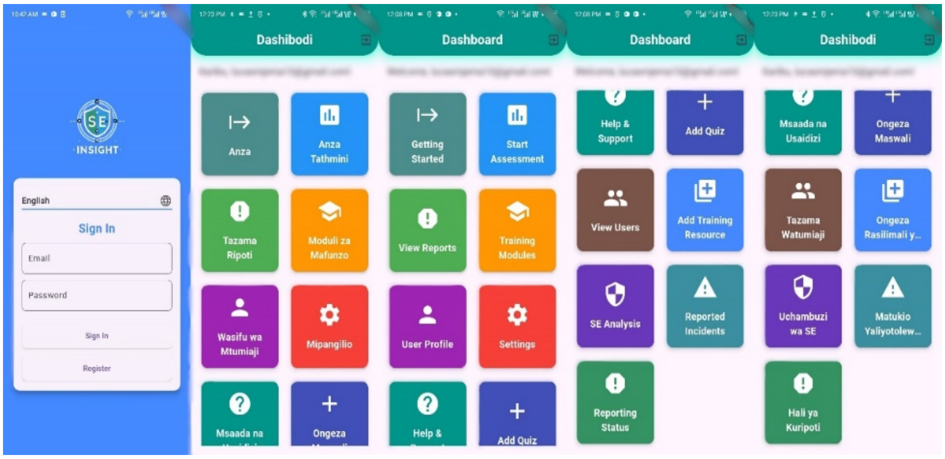
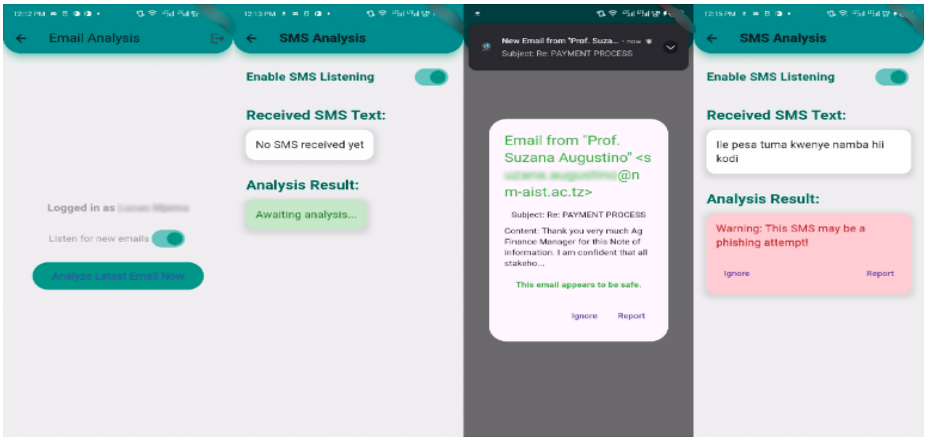


Figure 9. Login/Registration and Dashboard screens.

3.8.2. SE Analysis Screen (Email and SMS Analysis) and Analysis Result Screens

The Social Engineering (SE) Analysis Screen Module enables users to perform analysis on social engineering threats through both Email and SMS Analysis (Figure 10). The tool scans emails and SMS messages for indicators of phishing, smishing tactics. Users can turn on a switch to initiate a scan for every newly received email or SMS and the app provides instant results based on the analysis. After completing the analysis, users are presented with results that summarize potential threats found in either of the scanned email or SMS messages. The result screen on Figure 10 also offers a detailed breakdown of each threat and provides suggestions on whether to ignore or report the identified risks. The overall performance and recommendations are tailored based on the types of threats detected.



Email Analysis

Logged in as [redacted]

Listen for new emails

SMS Analysis

Enable SMS Listening

Received SMS Text:

No SMS received yet

Analysis Result:

Awaiting analysis...

New Email from "Prof. Suza... · now
Subject: Re: PAYMENT PROCESS

Email from "Prof. Suzana Augustino" <s[redacted]@nm-aist.ac.tz>

Subject: Re: PAYMENT PROCESS

Content: Thank you very much Ag Finance Manager for this Note of information. I am confident that all stakeho...

This email appears to be safe.

SMS Analysis

Enable SMS Listening

Received SMS Text:

Ile pesa tuma kwenye namba hii kodi

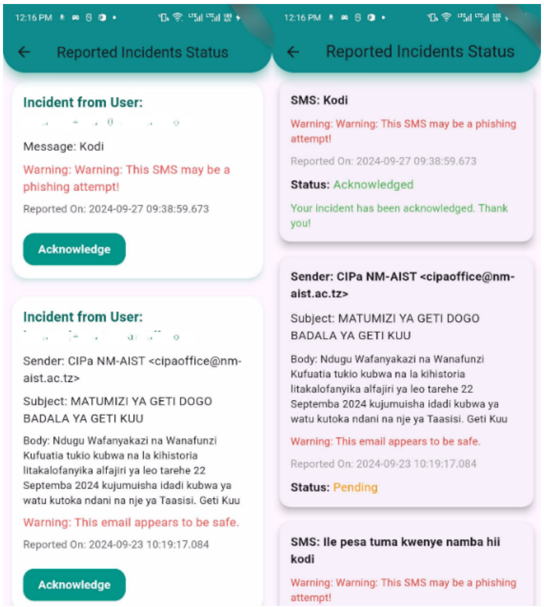
Analysis Result:

Warning: This SMS may be a phishing attempt!

Figure 10. SE Analysis and Analysis Results Screen

3.8.3. Reported Incidents and Reported Status Screens

The Reported Incident Screen allows admin to view all reported incidents of suspicious emails or SMS messages. Once an incident is reported, it is logged in the backend and made accessible to the admin for review. Users can track the status of their reports through the Reporting Status Screen, which displays whether the incident has been acknowledged or is still pending review. This functionality ensures that users can not only submit incidents but also stay informed about the progress and actions taken by the admin (Figure 11).



Reported Incidents Status

Incident from User:
[redacted]

Message: Kodi

Warning: Warning: This SMS may be a phishing attempt!

Reported On: 2024-09-27 09:38:59.673

Incident from User:
[redacted]

Sender: CIPa NM-AIST <cipaoffice@nm-aist.ac.tz>

Subject: MATUMIZI YA GETI DOGO BADALA YA GETI KUU

Body: Ndugu Wafanyakazi na Wanafunzi Kufuatia tukio kubwa na la kihistoria litakalofanyika alfajiri ya leo tarehe 22 Septemba 2024 kujumuisha idadi kubwa ya watu kutoka ndani na nje ya Taasisi. Geti Kuu

Warning: This email appears to be safe.

Reported On: 2024-09-23 10:19:17.084

Reported Incidents Status

SMS: Kodi

Warning: Warning: This SMS may be a phishing attempt!

Reported On: 2024-09-27 09:38:59.673

Status: Acknowledged

Your incident has been acknowledged. Thank you!

Sender: CIPa NM-AIST <cipaoffice@nm-aist.ac.tz>

Subject: MATUMIZI YA GETI DOGO BADALA YA GETI KUU

Body: Ndugu Wafanyakazi na Wanafunzi Kufuatia tukio kubwa na la kihistoria litakalofanyika alfajiri ya leo tarehe 22 Septemba 2024 kujumuisha idadi kubwa ya watu kutoka ndani na nje ya Taasisi. Geti Kuu

Warning: This email appears to be safe.

Reported On: 2024-09-23 10:19:17.084

Status: Pending

SMS: Ile pesa tuma kwenye namba hii kodi

Warning: Warning: This SMS may be a phishing attempt!

Figure 11. Reported Incidents and Reported Status Screens

3.8.4. Add Quiz and Add Training Module Screens

The Add Quiz Screen provides admins with tools to create and manage assessments (Figure 12). Quizzes can be added manually, one question at a time, or uploaded in bulk using a predefined template. Similarly, the Add Training Module Screen allows admins to upload training materials that will be made available to users in the training section. Admins can categorize training modules based on the type of social engineering threat they cover, ensuring that users have access to relevant and focused learning resources. Both screens streamline the process for admins to manage quizzes and training materials, enhancing the app's ability to adapt to evolving security challenges.

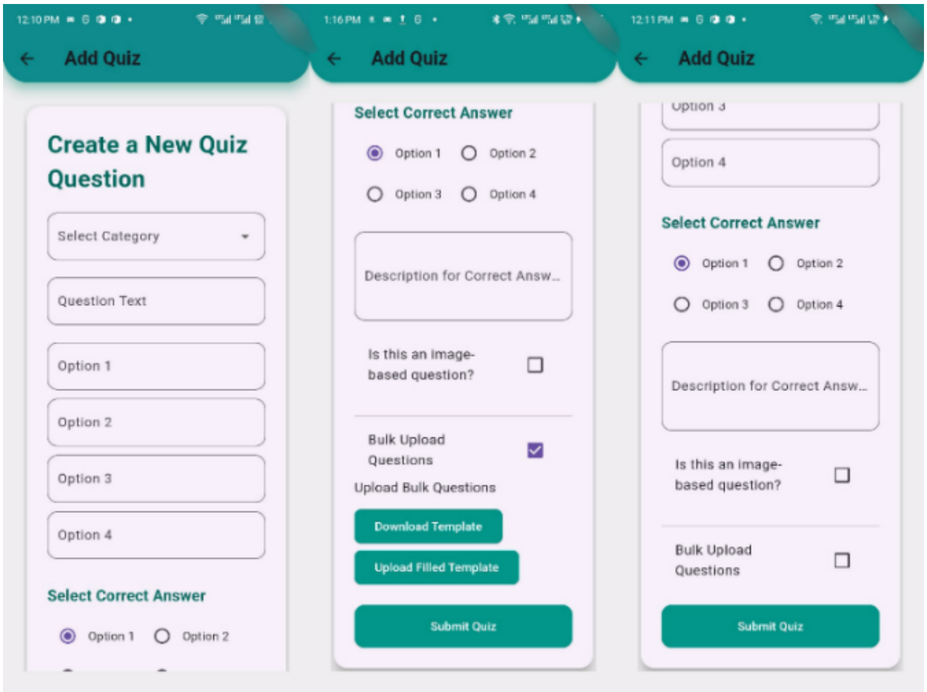
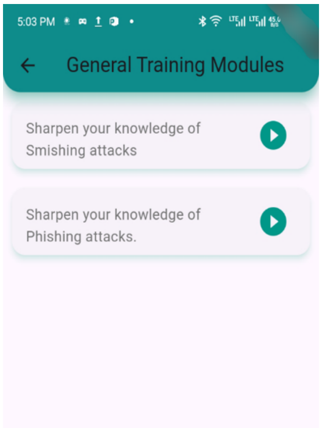


Figure 12. Add Quiz Screen

3.8.5. Training Module Screen

The Training Modules Screen provides users with access to educational materials aimed at increasing their understanding of social engineering threats (Figure 13). The training modules are categorized by threat type, allowing users to target specific areas where they may need additional learning. This section helps reinforce knowledge and prepares users to better recognize and report suspicious activity.



General Training Modules

Sharpen your knowledge of Smishing attacks

Sharpen your knowledge of Phishing attacks.

Figure 13. Training Module Screen

3.8.6. View Reports Screen Module

The View Reports Screen is a central interface for the admin (cybersecurity expert) and Head of ICT Department to monitor and manage the assessment performance and reported incidents across all users (Figure 14). This screen displays a summary of the assessments attempted by users, including individual scores, overall performance trends, and incident reporting statistics. In addition, the screen provides options for generating and downloading detailed PDF reports. These reports can be used for further analysis or documentation, making it easier for institutions to keep records of user performance and incident management over time. The View Reports Screen is designed to provide a comprehensive overview of the app's impact and the current state of social engineering awareness within the institution, serving as a crucial tool for evaluating the effectiveness of training and assessments.

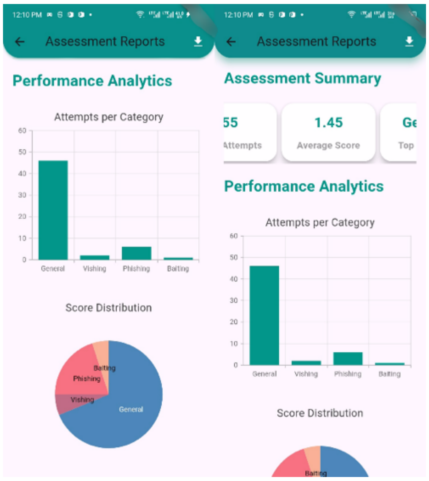


Figure 14. View Reports Screen

3.8.7. Pilot Testing and Feedback Integration

Following the development of the mobile-based tool, pilot testing was conducted with a group of 20 participants. This group included students, academic staff, and administrative staff, as the tool is intended for use by all of these roles within the institution. Feedback was collected through a user acceptance test, where participants performed specific tasks using the app and responded to a survey designed to measure ease of use, satisfaction, and effectiveness of the tool's features as seen in Figure 15. Feedback from participants was overwhelmingly positive, with 90% of users finding the app intuitive and easy to navigate. Participants also reported a significant increase in their awareness of social engineering threats after interacting with the app's assessment and training modules. Based on their feedback, several improvements were made to the tool, such as refining the incident reporting interface for clarity and adding more examples to the training module to cater to users with different levels of technical expertise.

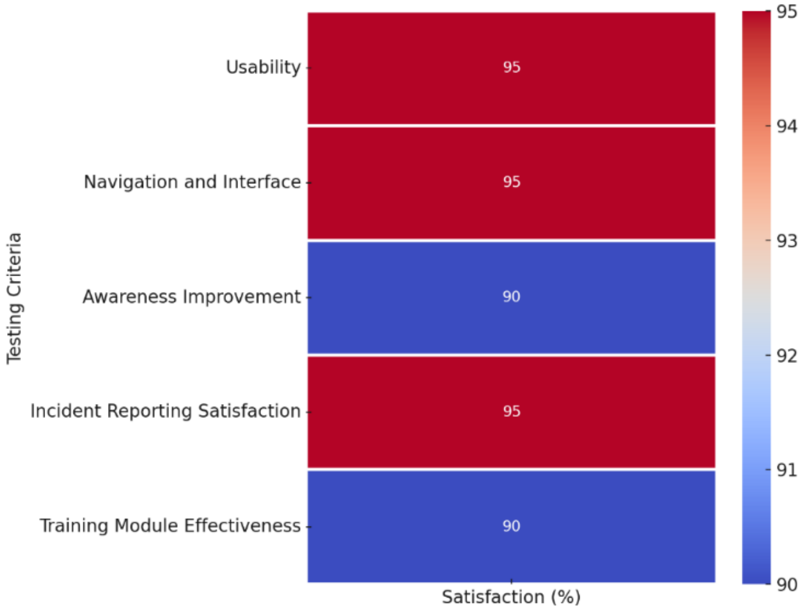


Figure 15. Pilot Testing and Feedback Integration

The results demonstrated that the mobile-based tool has strong potential to enhance social engineering awareness and reporting mechanisms in higher learning institutions. The feedback received from the pilot testing has been instrumental in refining the tool to meet the needs of its users, making it both intuitive and effective in addressing the gaps identified in current social engineering defenses.

3.9 Discussion

Social engineering attacks represent a critical cybersecurity challenge globally, with educational institutions being particularly susceptible due to typically decentralized IT environments and varying levels of user cybersecurity awareness. This study aimed to address this vulnerability gap specifically within Tanzanian higher learning institutions by developing a user-centric mobile-based application. Unlike previous initiatives primarily focused on traditional training sessions or passive instructional content, this tool uniquely combines real-time threat detection, personalized training, and simplified incident reporting capabilities directly accessible via mobile devices.

The findings from this study indicate strong user acceptance, demonstrated by an 85% reported improvement in participants' awareness of social engineering threats and a 90% satisfaction rating regarding ease of use. These findings align with previous research emphasizing the importance of user-friendly design and personalized content delivery in achieving lasting cybersecurity awareness. Additionally, our findings reflect previous insights that cognitive workload and user behavior significantly influence susceptibility to social engineering attacks [3], [4], suggesting that intuitive, low-cognitive-demand tools can notably enhance security awareness. Specifically, similar to the findings of Grobler et al. [11], personalized and interactive approaches significantly outperform static, generic training materials in engaging users and promoting sustained behavioural changes. One critical insight from the current study was the effectiveness of integrating bilingual support. Given that English proficiency varies widely among Tanzanian academic populations, the inclusion of Swahili content notably enhanced engagement and comprehension. This aligns with existing research that underscores the importance of language accessibility in cybersecurity education, particularly within multilingual contexts prevalent in developing countries [20][23][24]. Consequently, future studies or implementations in similar multilingual environments should prioritize bilingual or multilingual capabilities to maximize engagement and educational outcomes.

Another notable outcome was the positive response to the instant incident reporting mechanism. Traditionally, institutional responses to social engineering attacks have been reactive, delayed, or dependent on manual reporting channels, which often deter user participation. The developed mobile application overcame these barriers by enabling immediate, intuitive reporting directly from the user's mobile device. This aligns with Albishri and Dessouky's [25] recommendation for combining automated detection tools with user-friendly reporting interfaces to significantly enhance the efficiency of cybersecurity incident handling. The improvement in user willingness to report suspicious incidents (reported satisfaction rate of 90%) highlights the potential for mobile-based platforms to enhance real-time responsiveness, reducing the risk window and potential impacts of successful social engineering attacks.

Furthermore, this study illustrates the potential for broader adoption of mobile-based cybersecurity tools within other educational institutions in developing countries. Given common challenges such as limited resources, language diversity, and varying technological skills, the findings from this research provide a valuable model for institutions facing similar conditions. A scalable, cost-effective mobile application leveraging technologies like Flutter and Firebase can be readily adapted to similar environments, helping institutions build a stronger cybersecurity culture with minimal resource strain.

From a theoretical perspective, our study aligns with the Technology Acceptance Model (TAM), demonstrating high perceived usefulness and ease of use among participants. These dimensions significantly influenced the willingness of users to adopt and regularly use the application. Future research could leverage TAM further to analyse user engagement and acceptance over longer-term deployments and to explore potential refinements based on evolving user needs.

This research underscores the critical role of innovative, user-friendly, and contextually adapted technological solutions in addressing persistent cybersecurity vulnerabilities. By demonstrating practical feasibility and clear user acceptance, the study provides valuable insights for policymakers and institutional decision-makers considering similar implementations. Further studies are recommended to explore scaling the solution to larger institutional populations, integrating advanced machine learning capabilities, and assessing the tool's long-term impact on cybersecurity culture and practices.

4. CONCLUSION

This study successfully designed, developed, and evaluated a mobile-based application tailored to enhance social engineering awareness and streamline incident reporting among users in Tanzanian higher learning institutions. The application integrated key functionalities including personalized training modules, interactive assessments, bilingual support, and instant incident reporting for phishing and smishing threats. Results from pilot testing demonstrated substantial improvements in user awareness, with 85% of participants reporting a significant increase in their understanding of social engineering threats. Additionally, the intuitive interface and ease of use resulted in high user satisfaction, with 90% approving the incident reporting mechanism. The findings underscore the potential for mobile-based applications to effectively bridge critical gaps in cybersecurity awareness and incident response within academic institutions, particularly in resource-constrained contexts. The integration of real-time threat detection, personalized and bilingual content delivery, and immediate reporting capabilities differentiates this solution from traditional cybersecurity interventions, emphasizing a proactive, user-centric approach to cybersecurity. Future research should explore the integration of advanced machine learning and artificial intelligence techniques to enhance threat detection accuracy, adapt to evolving attack methods, and automate more sophisticated threat responses. Expanding the application's scope to incorporate voice-guided interactions could also increase accessibility, catering to a wider demographic. Moreover, broader deployment across various educational institutions and potentially other sectors would offer valuable insights into scalability and impact, contributing significantly to global cybersecurity policies and best practices.

REFERENCES

[1] N. Y. Conteh dan P. J. Schmick, "Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks," *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp. 11–19, 2016.

[2] F. Salahdine dan N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, Art. 89, 2019.

[3] G. Montanez et al., "Cognitive workload and social engineering susceptibility: A human-centered approach," *Hum.-Comput. Interact.*, vol. 35, no. 2, pp. 135–149, 2020.

[4] S. M. Albladi dan G. R. S. Weir, "User susceptibility to phishing attacks: The role of user behavior," *J. Inf. Secur. Appl.*, vol. 48, Art. 102352, 2019.

[5] E. Titis dan P. Stephens, "Analyzing cyber attacks and cyber security vulnerabilities in the university sector," *Computers*, vol. 14, no. 2, Art. 49, 2025.

[6] E. D. Kundy dan B. J. Lyimo, "Cyber security threats in higher learning institutions in Tanzania: A case of University of Arusha and Tumaini University Makumira," *Olva Acad.–Sch. Res.*, vol. 2, no. 3, pp. 1–38, 2019.

[7] M. E. Eltahir dan O. S. Ahmed, "Cybersecurity awareness in African higher education institutions: A case study of Sudan," *Inf. Sci. Lett.*, vol. 12, no. 1, pp. 1–9, 2023.

[8] S. Al-Janabi dan I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the Middle East," *J. Inf. Knowl. Manag.*, vol. 15, no. 1, Art. 1650007, 2016.

[9] M. E. Whitman, H. J. Mattord, dan A. Green, "Reducing cyber crime in Africa through education," *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Rhodes, Greece, 2022, pp. 1–6, doi: 10.1109/CSR54599.2022.9996274.

[10] A. A. Semlambo, D. M. Mfoi, dan Y. Sangula, "Information systems security threats and vulnerabilities: A case of the Institute of Accountancy Arusha (IAA)," *J. Comput. Commun.*, vol. 10, no. 11, pp. 1–17, 2022.

[11] M. Grobler, R. Gaire, dan S. Nepal, "User, usage and usability: Redefining human-centric cyber security," *Front. Big Data*, vol. 4, Art. 583723, 2021.

[12] H. Aldawood dan G. Skinner, "Social engineering: The science of human hacking in higher education," *Future Internet*, vol. 11, no. 4, p. 89, 2019.

[13] N. S. Safa, R. Von Solms, dan S. Furnell, "Information security policy compliance: Investigating the role of security awareness and psychological factors," *Comput. Secur.*, vol. 56, pp. 70–82, 2016.

[14] M. Bada, M. A. Sasse, dan J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behavior?," *Proc. Int. Conf. Cyber Secur.*, 2015.

[15] S. Allam, S. V. Flowerday, dan E. Flowerday, "Smartphone information security awareness: A victim of operational pressures," *Comput. Secur.*, vol. 42, pp. 56–65, 2014.

[16] K. Matyokurehwa, N. Rudhumbu, C. Gombiro, dan C. Chipfumbu-Kangara, "Enhanced social engineering framework mitigating against social engineering attacks in higher education," *Secur. Privacy*, vol. 5, no. 5, e237, 2022.

[17] J. Hobbs, "Cybersecurity awareness in higher education: A comparative analysis of faculty and staff," *Issues Inf. Syst.*, vol. 24, no. 1, pp. 159–169, 2023, doi: 10.48009/1_iis_2023_114.

[18] A. M. H. Al-Hakimi dan M. Hassan, "Anti-social engineering: The importance of social engineering awareness training web platform," *Proc. 2024 IEEE 15th Control Syst. Grad. Res. Colloq. (ICSGRC)*, pp. 35–40, 2024.

[19] H. Havenstein, "Gamified corporate training and its role in enhancing cybersecurity awareness," *J. Cybersecurity Train.*, vol. 18, no. 3, pp. 221–230, 2020.

[20] E. C. Cheng dan T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, p. 192, 2022.

[21] T. S. Yin, I. F. Kasmin, Z. M. Z. Abidin, dan H. Vasudavan, "Mobile application for cybersecurity education and awareness since COVID-19 pandemic," *Int. J. Data Sci. Adv. Anal.*, vol. 4, pp. 263–269, 2023.

[22] A. Alroobaea dan P. J. Mayhew, "How many participants are really enough for usability studies?," *Proc. Sci. Inf. Conf. (SAI)*, London, UK, 2014, pp. 48–56, doi: 10.1109/SAI.2014.6918171.

[23] F. T. Ngo, R. Deryol, B. Turnbull, dan J. Drobisz, "The need for a cybersecurity education program for internet users with limited English proficiency: Results from a pilot study," *Int. J. Cybersecurity Intell. Cybercrime*, vol. 7, no. 1, p. 2, 2024.

[24] Z. Wang, H. Zhu, dan L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021.

[25] A. A. Albishri dan M. M. Dessouky, "A comparative analysis of machine learning techniques for URL phishing detection," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 6, pp. 18495–18501, 2024.