Phishing Simulation as a Proactive Defense: A Customizable Platform for Training and Behavioral Analysis

Abdulrahman Alsaqer, Hussain Almajed, Khalid Alarfaj, Mounir Frikha
Department of Computer Networks and Communications, College of Computer Sciences and Information Technology,
King Faisal University, Al-Ahsa, 31982 Saudi Arabia

***Abstract*—Phishing is one of the most persistent threats, but a lot of awareness programs still use generic, static training. This paper fills in the gap identified above by existing studies through the introduction of a phishing simulation platform that provides personalized, role-based simulation with real-time behavioral tracking. It is a multi-channel delivery (Email, Short Message Service (SMS), (WhatsApp) and can dynamically generate messages using placeholders to simulate realistic attack scenarios. User interactions are visualized on an integrated dashboard to let organizations judge the individual's risk and provide immediate awareness feedback. Due to ethical restrictions, real user testing could not be performed, and the system was tested using simulated data found to work with a cloud-ready front end. The solution shows great potential for being adopted by enterprises due to its potential to adopt an approach towards cybersecurity training in a more adaptive and engaging way.**

***Keywords*—Phishing; simulation; awareness; analytics; cybersecurity**

I. Introduction

Phishing is among the most persistent and damaging of today's cyber threats, and it is responsible for a great deal of the world's data breaches and financial losses. Data from recent studies shows that more than 30 percent of cyber security attacks and billions are lost owing to credential thefts, ransomware, and fraud [1], [2]. Phishing persists even though organizations make investments in technical defenses such as email filters, spam detectors, and firewalls since they leverage the human element, including trust, emotion, and behavioral habits [3], [4].

Generic security awareness training provided by most organizations rarely changes user behavior or provides a contextual learning experience [1], [5]. These methods ignore individual vulnerabilities as well as fail to validate the simulation of realistic attack scenarios. Traditional training methods have been found to be ineffective in stopping users from clicking on links to phishing [2].

Phishing simulations are a more dynamic and effective way to address these gaps. Simulations are used by simulating real-world attacks in a controlled environment in order to build awareness and help the users produce proper responses to the threats [6], [3]. However, most of the existing platforms only support email phishing, do not support mobile-based attacks such as SMS or WhatsApp phishing, and do not collect or analyze user behavior for adaptive training [4], [7].

We further propose a new approach, which is a customizable, multi-channel phishing simulation platform with behavioral analytics. Our platform is unlike conventional tools as it supports simulation through email, SMS, and WhatsApp and tracks user interactions in terms of response time, clicks, and risk metrics as per role. Motivated by recent research, we propose a platform that makes cybersecurity training more appealing, adaptive, and conforming to the actual needs of an organization.

A. Background on Phishing Threats and their Evolution

Phishing is a deceptive scheme employed by cyberattackers who manipulate users into providing sensitive information to them, such as login credentials, financial information, personal information, etc. Fig. 1 illustrates an overview of phishing attacks. In the past, phishing was more dependent on poorly written emails with generic messages and links that were suspicious. However, these early attacks were easy to detect because there were visible red flags such as spelling errors and strange formatting [3]. Phishing has now become more complex and a multi-channel threat.

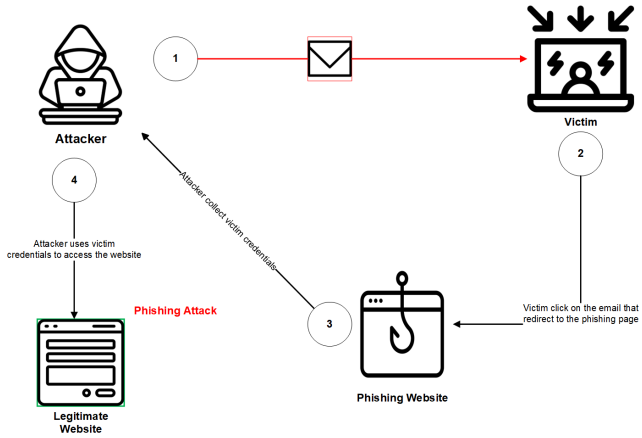

Fig. 1. Overview on phishing.

Phishing campaigns have gone beyond email and now involve SMS (smishing), social media platforms, messaging apps such as WhatsApp, and even phone calls Voice phishing (Vishing) to reach users in more personalized ways [6], [7]. Email spoofing, brand impersonation, and the use of HTTPS-secured malicious websites bring the ability to distinguish

between legitimate and fraudulent communications to the level of sophistication [4], [8]. This evolution of spear phishing takes the next step by sending a tailored message to a specific person based on his/her job role, behavioral patterns, or personal information scraped from public sources [1], [2].

All these advancements make it increasingly easy for phishing attacks to appear more convincing and more difficult to detect, even for a trained group. Psychological triggers, such as urgency, authority, or fear, are being increasingly used by attackers to induce an immediate action without critical thinking [3], [2]. Phishing methods are changing all the time to get around technical filters and to exploit human vulnerabilities, and traditional security measures are not enough. Finally, it is necessary for organizations to adopt proactive, scenario-based training models that resemble actual attack patterns and focus on the behavior of the users [5], [9].

B. Behavioral Importance and Limitations of Current Awareness Training

With the advancement of technical defense such as firewalls, intrusion detection systems, and anti-phishing filters, the attacks of phishing are still going on and thrive due to human nature, not the system itself. In fact, we know from studies that employees still remain vulnerable to phishing emails and clicking malicious links by habit, curiosity, or urgency even after formal training sessions [1], [3]. Because human decision-making is complex and unpredictable, it is difficult to 'patch' users like one would patch the software vulnerabilities.

Common awareness programs, on the other hand, operate on the basis of one-time, passive training modules that do not adapt to a changing threat or lead to practicing good security habits [5]. Typically, these programs are rushed through or forgotten and have limited long–term impact on user behavior [3]. On the other side, interactive and ongoing training approaches, especially phishing simulations, have been more effective in creating user awareness and response [5], [4]. Organizations can provide experiential learning through the simulation of real-world attack scenarios, reinforce the correct response, and immediately provide feedback on mistakes through the simulation.

Most importantly, behavioral-based training allows organizations to monitor user engagement, identify risky behavior patterns, and push targeted interventions to the highest-risk users [1], [9]. Because phishing attacks have become more targeted and more realistic, having a human firewall in place is more important than ever and means adaptive training is key. The shift from compliance-based awareness to behavior-driven education is the one that will not only help to build organizational resilience to social engineering threats but also other types of security threats [5], [9].

C. Purpose of the Study

This study aims to develop a customizable phishing simulation platform based on the limitations of traditional phishing awareness programs that deliver realistic, multi-channel attack scenarios and analyze users' behavior to improve the training outcome. Unlike static training, this platform will interact with users through simulations sent through email, SMS, and WhatsApp, which mimic real-world phishing vectors. It also includes behavioral analytics that tracks user actions, including click rates, response times as well as reporting behavior. These insights could be leveraged to provide subsequent training with a basis in individual risk profiles such that high-risk users are supported. This study combines simulation, customization, and behavioral analysis to offer proactive, adaptive, and user-centric solutions that improve organizational resilience against phishing attacks.

D. Research Questions

The following research questions are formulated to guide the development and evaluation of the proposed phishing simulation platform.

- RQ1: What are the effects of phishing simulations on long-term cybersecurity awareness and a decrease in risky user behaviors?
- RQ2: When phishing attacks that simulate an environment are devised, what communications and behavioral patterns emerge, and how can such patterns be used to create personalized training exercises for those individuals?
- RQ3: What makes a customizable simulation platform better than one generic simulation fit for all awareness programs in terms of engagement as well as learning outcomes?
- RQ4: What difference does user engagement and threat recognition of a mobile phishing simulation (such as SMS, Whatsapp) compare to an email phishing simulation?
- RQ5: What are effective methods for using behavioral analytics and real-time feedback to change the phishing training approach as well as enhance long-term awareness and response accuracy?

The current paper explores the structure of the system and experimental application of simulated data. Subsequent stages will be real-user validation.

E. Paper Structure

The rest of this paper is organized as follows: Section II first reviews related work and then describes the limitations of existing phishing awareness solutions. In Section III, research methodology and the process to identify the system requirement is described. In Section IV, the proposed solution is presented along with system objectives and architectural overview. In Section V, the system design is detailed with diagrams, components and workflow. In Section VI, the system's contribution to the research questions is discussed. Section VII discussed key challenges met during the development. The paper concludes in Section VIII and describes the future work directions.

II. Literature Review

In order to get a more effective solution, there are recent developments that must be understood within the realm of phishing awareness and simulation-based training. Twelve studies were reviewed as relevant that were published between

2021 and 2024. The number of publications grew in the year 2022, as shown in Fig. 2, which shows that phishing detection and user-focused cybersecurity training is receiving increased academic interest. This paper suggests the strengths and limitations of existing approaches with an emphasis on simulation techniques, analysis of user behavior, and delivery through the multi-channel. The results of this review guided the design decisions for the proposed phishing simulation platform.

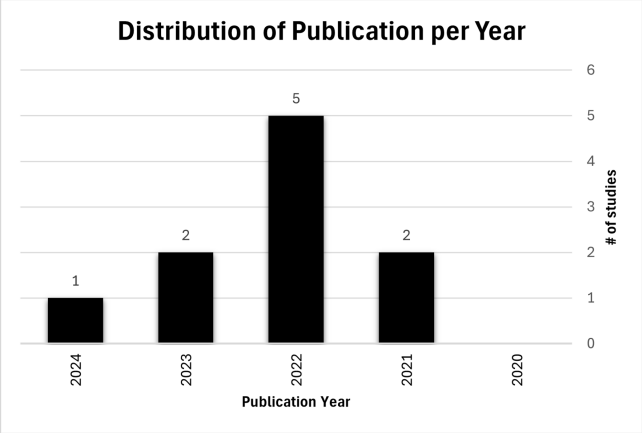

Fig. 2. Papers per year of publication.

Yeng et al. [10] develop a framework for exploring incentive-based methods to reduce phishing susceptibility in the healthcare sector through a review and in-the-wild simulation. The authors analyzed 16 tools and six previous simulation studies using hybrid methodologies combining surveys and field tests. Findings highlight the dominance of deception-based phishing, where employees responded most to simulated attacks involving malicious links. However, the research reveals that while behavioral theories like protection motivation have been examined, incentive-based strategies remain largely unexplored. Ethical concerns were prominent, especially regarding deceptive simulations. Although the framework provides practical direction for future training implementations, the study is limited by its lack of real-world validation of incentive models. This reveals a clear gap: existing healthcare phishing simulations do not incorporate adaptive, personalized, or multi-channel behavioral incentives.

Sutter et al. [11] investigate influential factors of phishing awareness training by analyzing over 31,000 participants across 144 phishing simulations. It introduces a data-driven machine learning model that predicts email difficulty perception using structural and Natural Language Processing (NLP) features. Results show that most users avoided credential-based phishing after 12 weeks of training and that user-specific training is more effective than broad, group-based approaches. The model enables pre-deployment assessment of email "convincing power," addressing a key challenge in designing fair simulations. However, the study is limited to email-based vectors and lacks long-term behavior tracking. While it advances adaptive difficulty estimation in simulations, it does not extend beyond email, omits behavioral logging, and offers no user feedback customization.

Ahmad et al. [12] presents a web-based phishing simulation platform integrated with embedded learning tools to enhance user awareness and real-time response. The system includes user roles, scenario-based phishing modules, and a database-backed structure that enables immediate engagement during simulated attacks. Through iterative testing and deployment, the study demonstrates significant improvement in users' ability to detect phishing attempts. Embedded learning — training users in the context of their actual digital environments — proves more effective than standalone awareness sessions. However, the study focuses exclusively on email phishing and does not include data on user behavior patterns post-training or adaptivity based on user history. This gap emphasizes the need for customizable, behavior-tracked multi-channel simulations.

Kävrestad et al. [13] evaluates the effectiveness of two phishing awareness training methods—game-based learning and Context-Based Micro-Training (CBMT)—through a simulated experiment using eye-tracking. Participants were asked to detect phishing emails before and after undergoing training. Results show that CBMT, which delivers short and relevant content at the moment of need, led to more secure user behavior than game-based learning. Nonetheless, despite training, many participants still failed to identify phishing attempts, highlighting that training alone is insufficient. The research is limited in scale and scope, focusing solely on desktop-based email simulations with no integration of adaptive or personalized feedback. This reinforces the research gap addressed in the current work: the need for a multi-channel, customizable phishing simulation system that integrates behavioral analytics and adaptive interventions beyond static training formats.

Chatchalermpun and Daengsi examine the use of simulated phishing attacks to improve cybersecurity awareness among users in a real-world training context [14]. Conducted as a case study, the simulation helped measure participants' susceptibility and learning outcomes following exposure to various phishing email templates. The study highlights increased awareness and reduced click rates post-simulation, suggesting that experiential exposure is beneficial. However, the simulation was limited to credential-based email phishing and did not assess behavioral change over time or account for alternative phishing channels such as SMS or voice. Moreover, the system lacks embedded feedback mechanisms or personalization. These limitations underscore the importance of developing a simulation environment that not only mimics real attacks but also tracks behavioral metrics and offers adaptive content across multiple platforms, as proposed in this research.

Canham et al. [15] introduce Phish Derby, a gamified phishing awareness initiative conducted at a U.S. university designed to explore employee motivation and reporting behavior in phishing simulations. Participants competed to detect phishing emails, with rewards incentivizing participation. Key findings reveal that prior simulation performance, age, and device consistency influenced reporting accuracy. Interestingly, users with high extraversion or agreeableness scored lower, while those with a learning-oriented mindset underperformed compared to reward-driven peers. The study effectively highlights how individual traits affect detection performance. However, it is narrowly focused on desktop email reporting and omits broader behavior tracking or multi-platform phishing vectors. The absence of post-simulation adaptive learning or customizable challenge levels marks a

research gap that this project addresses through its dynamic, behavior-aware simulation design.

Tinubu et al. [16] introduces PHISHGEM, a mobile game-based learning application developed to promote phishing awareness through interactive gameplay. The game engages users in scenarios that mimic phishing attacks, requiring them to identify deceptive messages and make real-time decisions. Evaluations show significant improvements in user awareness, particularly among younger participants with high mobile engagement. The gamified approach enhanced motivation and retention, suggesting a promising direction for immersive learning tools. However, the study is limited to mobile platforms and does not capture longitudinal behavioral data or cross-channel phishing patterns. Additionally, the training lacks real-world simulation integration and adaptive feedback. These omissions highlight the need for a multi-device, behavior-tracked platform—an aspect central to the proposed research's focus on customizable, context-aware simulation environments.

Yeoh et al. [17] presents a combined approach using simulated phishing attacks and embedded training to raise awareness among organizational users. The campaign involved multiple simulation rounds, each followed by immediate educational interventions within the user's workflow. This embedded model led to measurable reductions in click-through rates and improved user recognition of phishing content over time. The study emphasizes the effectiveness of just-in-time learning, contextual reinforcement, and iterative exposure. However, the scope is confined to email-based simulations and lacks adaptability to individual behavior or phishing variants beyond email, such as voice or SMS. Furthermore, it does not log behavior traits or personalize content delivery. These limitations reinforce the necessity for an adaptive, multi-channel training model with behavioral analytics, which this research aims to introduce.

Ciupe and Orza report on a large-scale phishing simulation conducted at a higher education institution involving over 20,000 users [18]. The campaign used multiple social engineering tactics delivered via Office 365 services, simulating realistic attacks to evaluate click rates, report behaviors, and user confidence. Results indicate a varied level of cybersecurity awareness, with participants showing inconsistent ability to detect phishing attempts. The study emphasizes the value of experiential learning and reflective feedback but acknowledges the ethical challenges of covert simulations and the limitations of one-size-fits-all training. Importantly, the simulation lacked multi-channel attack vectors, behavioral tracking, and individualized training paths. These gaps underscore the importance of customizable and adaptive simulations with analytics-based feedback loops.

Rizzoni et al. [19] analyze phishing simulations conducted in a large Italian hospital with over 6,000 staff members. Three campaigns were launched, comparing responses to generic versus customized phishing emails. Results showed a markedly higher success rate for personalized attacks, demonstrating that contextual cues significantly influence user susceptibility. The study stresses that phishing simulations can be effective but also complex to execute, particularly in sensitive environments like healthcare. Challenges included operational disruptions, resistance from staff, and ethical concerns about using deception. While it confirms the value of customization in phishing training, the study was restricted to static email scenarios and lacked any adaptive learning paths, post-simulation behavior tracking, or integration with non-email phishing vectors such as SMS or voice. These omissions highlight critical limitations that the current research addresses through its proposed dynamic, multi-channel, and behavior-aware simulation framework.

Table I shows the summary of existing works in phishing simulation.

TABLE I. SUMMARY OF REVIEWED PHISHING SIMULATION STUDIES AND IDENTIFIED GAPS

Paper	Objectives	Identified Gap	Method Used
Yeng et al. [10] (2023)	Incentive-based email phishing simulation in healthcare.	Lacks adaptive training and multi-channel support.	Email-based phishing
Sutter et al. [11] (2022)	Email difficulty prediction model using machine learning.	No behavioral tracking; email-only channel.	Email-based phishing
Ahmad et al. [12] (2023)	Embedded simulation tools with real-time feedback.	No user behavior adaptation; lacks mobile simulation.	Email-based phishing
Kävrestad et al. [13] (2022)	Eye-tracking study comparing contextual micro-training and games.	No role customization; no long-term behavior analysis.	Email-based phishing
Chatchalermpun and Daengsi [14] (2021)	Real-world email-based simulation campaign.	No feedback personalization; no multi-channel phishing.	Email-based phishing
Canham et al. [15] (2022)	Gamified competition to improve phishing reporting.	No adaptive content; email-only; no analytics integration.	Email-based phishing
Tinubu et al. [16] (2022)	Mobile game for phishing awareness and education.	Lacks behavioral tracking and role-based simulation.	Mobile game-based
Yeoh et al. [17] (2021)	Embedded training after phishing simulations.	No adaptivity or multi-channel simulation.	Web-based email phishing
Ciupe and Orza [18] (2024)	University-wide phishing simulation via Office 365.	Static training content; no personalized feedback.	Web-based email phishing
Rizzoni et al. [19] (2022)	Phishing simulation in a hospital using custom messages.	No behavior tracking or dynamic learning; ethical constraints.	Web-based email phishing

III. RESEARCH GAP AND CONTRIBUTION

Despite increased interest in phishing awareness strategies, current literature continues to reveal foundational limitations that hinder effective long-term defense.

1) Limited multi-channel phishing simulations: Most studies focus exclusively on email-based phishing simulations, overlooking other attack vectors such as SMS and messaging platforms commonly exploited by modern attackers.

2) Short-term awareness measurement only: The majority of studies evaluate user awareness immediately after simulation or training without assessing long-term retention or behavioral change over time.

3) Lack of targeted phishing training for diverse workforce types: Existing platforms and studies often adopt a one-size-fits-all model, failing to deliver tailored simulations or feedback based on role, risk exposure, or behavioral patterns.

A. Contribution

This research addresses the above gaps by developing a next-generation phishing simulation platform with the following contributions:

1) Extending beyond email: The platform supports phishing simulations across Email, SMS, and WhatsApp, reflecting the evolving multi-channel nature of phishing threats.

2) Customization for diverse needs: The system enables simulation customization based on organizational roles and contextual risks, providing more relevant and effective training experiences.

3) Holistic, proactive training: By combining real-time phishing simulations with behavioral insights and feedback, the platform supports continuous learning and improved cybersecurity readiness.

IV. Proposed Framework

In order to address the identified limitations in existing phishing training systems, this section proposes a framework for a customizable phishing simulation platform. Phishing simulation across multiple communication channels (Email, SMS, WhatsApp) intends to collect user interaction data and provide behavior-based feedback. This constitutes the conceptual basis for system implementation and evaluation. The framework is built around four main components: simulation design, message delivery, behavior tracking, and adaptive training.

A. Objectives

The main goal is to develop a Comprehensive, customizable, and behavior-aware phishing simulation framework that is inclusive of traditional limitations of existing phishing awareness training methods. Specifically, the framework aims to:

1) Simulate multi-channel phishing attacks: Deliver many realistic phishing attack scenarios via delivery channels of Email, SMS, and WhatsApp, just as an attacker would do today.

2) Enhance user awareness through real-time feedback: Redirect users that interact with phishing links immediately to awareness pages that have educational content relating to the type of attack, thus enhancing learning retention and behavioral change.

3) Track and analyze user behavior: Observe user interaction and log user interaction such as click activity and response time to know the phishing susceptibility and behavioral trend of the user.

4) Support role-based simulation targeting: Allow for customizing simulations by organizational role to allow training to be more relevant to the user's context of work and risk exposure.

5) Classify risk based on role clicks interaction: The organization's performance is categorized as per the risk levels like high, medium, and low, and identifies which role may need more training.

6) Generate actionable reports for administrators: To provide detailed analytics and reports via a centralized dashboard to help plan all the campaigns for security teams to track campaign performance, compare role-level results, and make a decision.

7) Design for scalability and future integration: It creates a framework that is made modular and extendable enough so that new attack vectors or learning mechanisms can be integrated in the future

B. System Design

The creation of a phishing simulation platform is based on modularity, scalability, and tracking of behavior. The system is composed of several components that, when combined, provide users with the ability to send simulated phishing attacks, capture user responses, and generate reporting. It ensures separation between the admin functionalities, simulation engine, tracking mechanism, and awareness content.

C. Context Diagram

A high-level overview of the core entities involved in the phishing simulation platform and their interactions are provided by the context diagram. It focuses on how the administrative action, user action, and message delivery process operate on the system. As shown in Fig. 3 there are three main entities that the system interacts with:

1) Administrator: It creates user roles, adds users, designs phishing templates, configures simulation campaigns, and initiates simulation runs to manage the system. Upon execution, the admin gets statistics and behavioral data for analysis.

2) Target users: The system sends phishing messages to you through email or SMS. If a phishing link is clicked, they are redirected to an awareness page, and their interactions (e.g., clicking links, time-to-response) are monitored.

3) Mobile and email channel Application Programming Interface (API): Acts as a delivery mechanism for sending phishing messages across multiple communication channels. It handles message dispatch requests from the system and returns delivery status updates.

The Phishing Simulation Awareness System manages all logic inside of the system, ranging from template customization, tracking link generation, data logging, user behavior analysis, and real-time redirection to awareness pages.

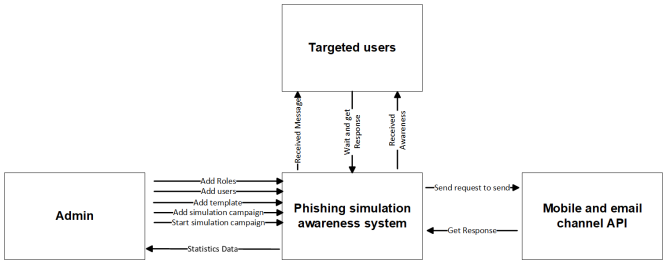

Fig. 3. Context diagram of the phishing simulation awareness system.

D. Use Case Diagram

The functional overview of the use case diagram answers the question of how the primary actors, which are the administrator and the targeted user, interact with the phishing simulation platform. The system is described from campaign configuration through to user interaction all the way to delivery of user feedback.

Fig. 4 shows the use case diagram, and the administrator responsibilities are listed in Table II.

TABLE II. ADMINISTRATOR USE CASES

Functionality	Description
Manage Roles	Decide what different user groups (e.g., Sales, Marketing) should be able to simulate.
Manage Users	Set and assign users to pre-defined roles for campaign targeting.
Manage Templates	Build Email, SMS, and WhatsApp phishing templates for delivery along with placing holder to substitute with a link generated by the system and a targeted user name.
Create Campaigns	Create phishing simulations and link them to roles.
Launch Simulation	Initiate an immediate phishing simulation.
View the Campaign List and Details	Check on all current and past campaigns with status updates.
View Tracking Data	Look into link clicks and response times of users.

The targeted user responsibilities are listed in Table III.

TABLE III. TARGETED USE CASES

Functionality	Description
Receive Message	The assigned communication channel is used to message users with phishing messages.
Click the Link	on the interaction with the phishing link, the user behavior is tracked.
View Awareness Page	Upon clicking a phishing link, the user is automatically directed to an awareness page for immediate feedback.

From this diagram, the system will cover all functional requirements of the system as well as support interaction between administrative users and end-user participants.

E. System Architecture

The proposed phishing simulation platform uses a layered and modular architecture to make sure that the system is scalable, maintainable, and secure. As depicted in Fig. 5, the system consists of many interconnected components that are partitioned into six key layers.

1) Frontend layer – admin dashboard: Administrators have a secure, web-based interface to this layer. It enables:

- User and role management.
- Template design.
- Campaign creation and tracking.
- Real-time navigation across simulation statistics.

The dashboard is constructed by modern web technologies and hence responds and provides intuitive interaction.

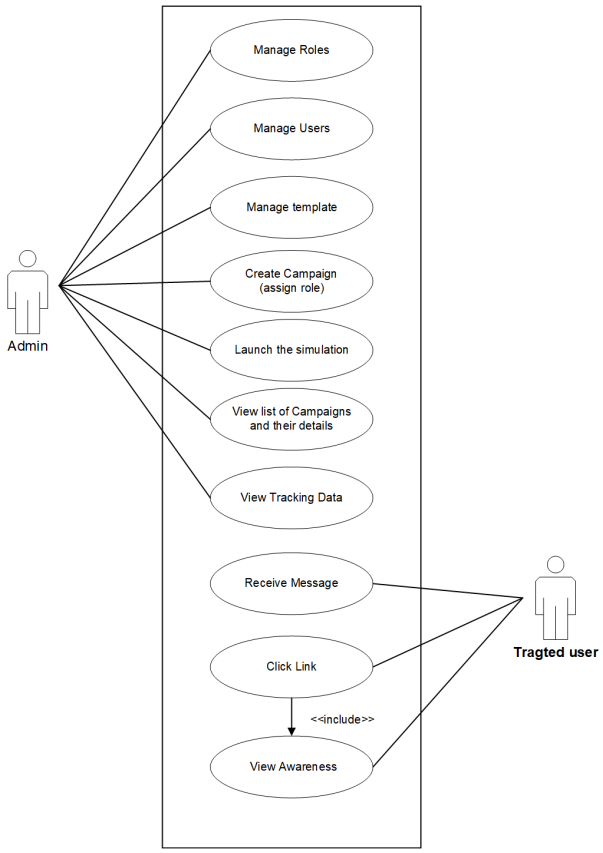

Fig. 4. Use case diagram of the phishing simulation platform.

2) Backend logic layer: Implemented using React.js, this layer:

- Handles campaign logic.
- Creates a unique phishing link for each user template pair.
- Logs user activity (clicks, timestamps).
- Assigns behavior-based risk scores.

3) Communication API layer: It is responsible for sending phishing messages via using resend API for sending email and looking for SMS and Whatsapp.

This layer communicates with the backend, acting as a middle layer to dispatch phishing content and log delivery status using a secure request-response mechanism.

4) Tracking engine:

- It creates individualized URLs for every user.
- To capture the users' actions, such as response time and frequency of clicks.

5) Awareness module: In case of a user interaction with a phishing simulation:

- This redirects them to a tailored awareness page.
- The page provides microlearning content or training tips delivered just in time to reinforce security behavior.

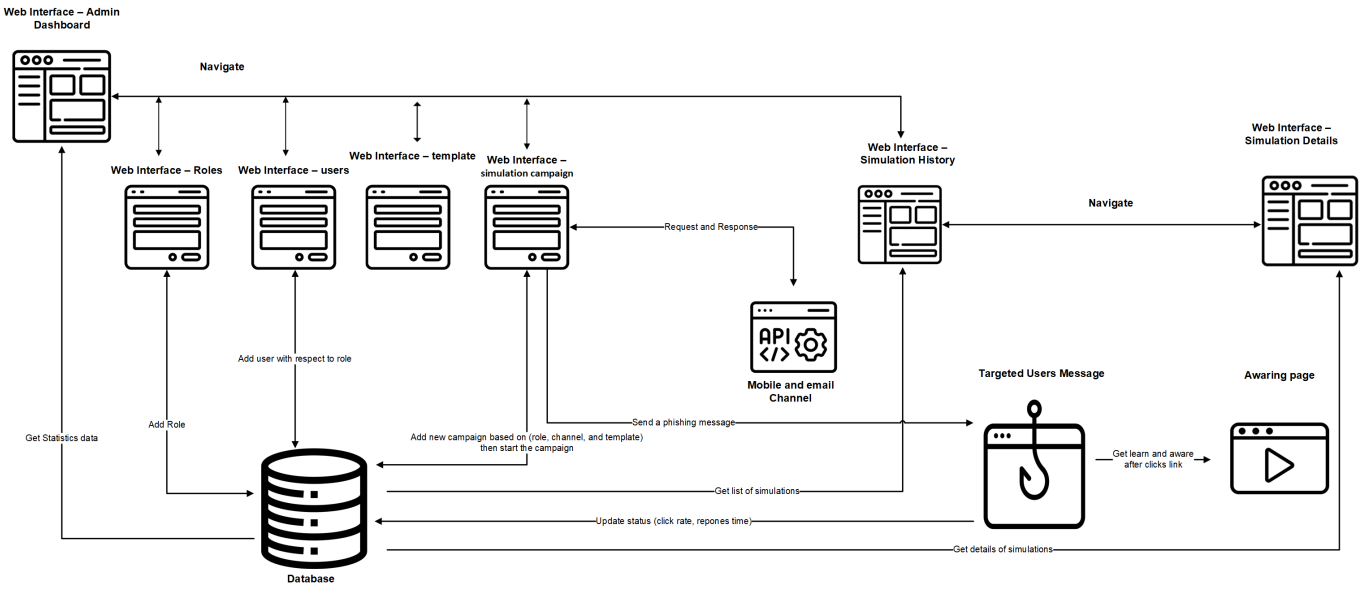

Fig. 5. System architecture of the phishing simulation platform.

6) Database layer: All simulation data, including is stored and secured on the system.

- User roles and profiles.
- Campaign settings and templates.
- Click activity and behavioral logs.

F. Database Design

Designing the database for the phishing simulation platform is based on the normalized relational model to ensure data integrity, efficient querying, and scalability. It is capable of catching main entities like users, roles, simulations, templates, and behavior tracking. In this section, we present an Entity Relationship (ER) model at a high level, as well as the corresponding relational schema to be used for the implementation.

1) ER Diagram: As shown in Fig. 6, the logical structure of the data used in the simulation system is modeled by the ER diagram.

Table IV captures the key relationship between the entities involved.

TABLE IV. THE RELATIONSHIPS BETWEEN KEY ENTITIES.

Entity	Goal
Users	those who are phished in phishing simulations. A user can be assigned to one of the roles.
Roles	Determine user categories (e.g., HR, IT) to target for simulation.
Phishing Templates	Using pre-defined messages for each campaign based on their type and delivery channel.
Simulations	The admin will create a campaign using templates and targeting specific roles.
Simulation Tracking	Tracking individual users' interactions with phishing simulations (delivery status, response time, and click behavior).

Key relationships include:

TABLE V. PHYSICAL IMPLEMENTATION OF THE PHISHING SIMULATION DATA MODEL WITH PK AND FK RELATIONSHIPS

Table	Role
Users	Contains basic user details along with the details of role association.
Roles	The definition of roles used to group users.
Phishing Templates	Stores the message content, channel type, and creation date.
Simulations	Metadata about the campaign, including channel, name, and the link to templates.
Simulation Tracking	Records user responses in the form of click_time (initial NULL value), track_id, and delivery status.
Simulations_Targets	Connects simulations to targeted roles.

- One-to-many relationship between Roles and Users.
- Many-to-one between Simulations and Templates.
- Users and Simulations, they are many-to-many relationships, and we will resolve this through Simulations Tracking.

2) Database schema diagram: Fig. 7 illustrates the way the ER model is implemented using the Structured Query Language (SQL) relational tables. It describes what the data types are, the Primary Keys (PK) and Foreign Keys (FK) throughout the system.

The schema adheres to the normalization principles of the Third Normal Form (3NF), aiming at eliminating redundancy and ensuring relational consistency. It makes possible user performance tracking, report generation, and behavior analysis at individual and group levels. Table V represents the tables and role of each for the system.

G. Workflow Diagram

The phishing simulation platform is a streamlined, direct execution workflow that keeps administrators able to initiate

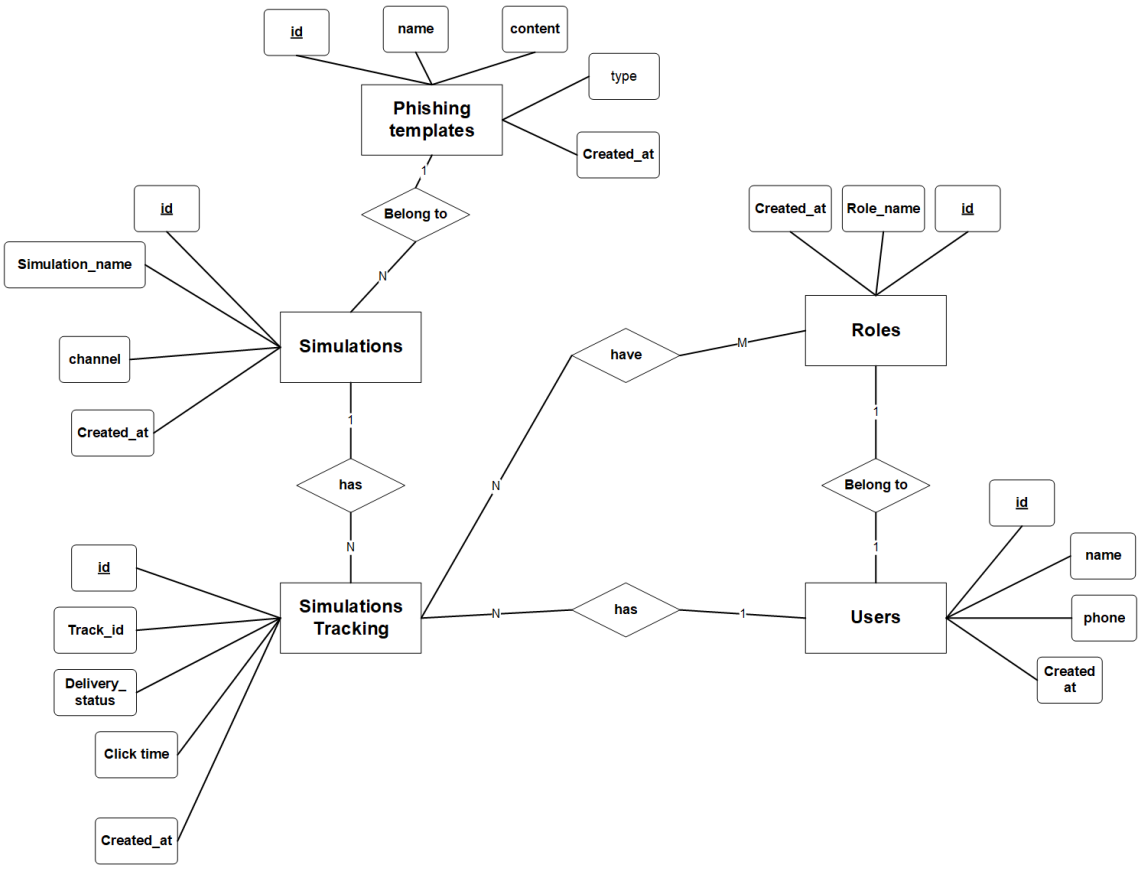

Fig. 6. ER Diagram of the phishing simulation system.

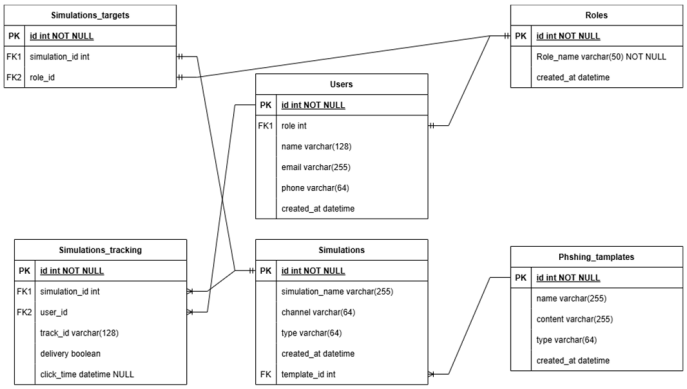

Fig. 7. Database schema diagram of the phishing simulation system.

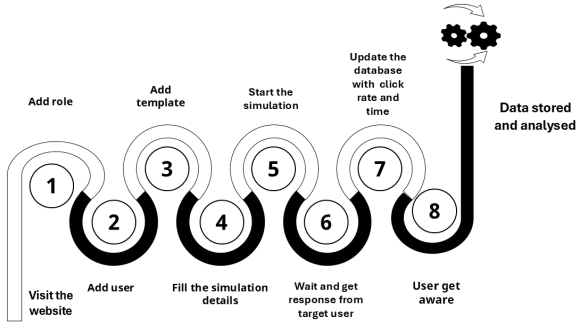

Fig. 8. System workflow of the phishing simulation platform.

and monitor phishing simulations without much delay in configuration. The workflow shown in Fig. 8 details the workflow as eight steps in succession: administrative setup, campaign launch, user interaction, and behavior tracking.

1) Step-by-step workflow:

a) System access: The process is initiated by logging into the platform via a secure web interface by the administrator.

b) User registration: User profiles are set up and assigned to pre-defined (organizational) roles like HR and Finance so that specific simulations can be run against them.

c) Template configuration with placeholders: Phishing templates with dynamic placeholders are created by the administrator. The backend system automatically replaces these placeholders at runtime.

- {{user_name}}: Replaced with the targeted user's name.
- {{tracking_url}}: Replaced with a unique tracking link generated for the user-template pair and simulation campaign.

- {{random_number}}: Generate a random number (Fake invoice or verification code etc).

Using this mechanism allows a simulation to be more realistic and more personalized, thus making it more effective in emulating real phishing attempts.

d) Simulation setup: By selecting a template, delivery channel, and target user groups (roles), it is the admin who configures the simulation. It is saved and immediately ready for launch.

e) Immediate campaign execution: Once the backend is launched, it dynamically fills in the placeholders with actual values and dispatches the phishing messages through Email, SMS, or WhatsApp API. A customized message with a user's personal data and a unique tracking link is sent to each user.

f) User interaction logging: The system records user actions including: delivery status, link click events, and time to response.

g) Behavioral data collection and risk scoring: The data of user interaction is stored in the database. For instance, the system calculates risk scores and classifies an organization's risk level according to predefined thresholds.

h) Awareness feedback delivery: Upon interacting with phishing links, users are redirected to a training page with immediate awareness content. The reinforcement of learning through real-time feedback and behavioral reinforcement is reiterated by this step.

This is a behavior-focused and fully dynamic workflow that allows for the multi-channel delivery of phishing simulations. It makes use of placeholders to increase the realism of messages and its supportable and scalable deployment.

V. System Implementation

Thereafter, the phishing simulation platform was implemented by translating the proposed architecture and system design into a working web-based system. The development took a modular approach to allow for each component to be developed, tested, and improved independently: user management, template creation, simulation launch, behavior tracking, and reporting.

A. Technology Stack

Table VI shows the tools and technologies used for building the platform.

TABLE VI. List of Tools and Technology

Component	Technology / Tool
Backend Development	React.js
Frontend Development	HTML and CSS
Database	PostgreSQL
Message Delivery APIs	resend API for email
Development Environment	Visual Studio Code
Diagram Modeling	Microsoft Visio and draw.io.

B. Development Modules

Several modular components were used to implement the platform, and each module plays a particular role in the phishing simulation workflow.

- Admin Dashboard: Fig. 9 shows the web interface for administrators to navigate users, roles, other interfaces, and review reports.

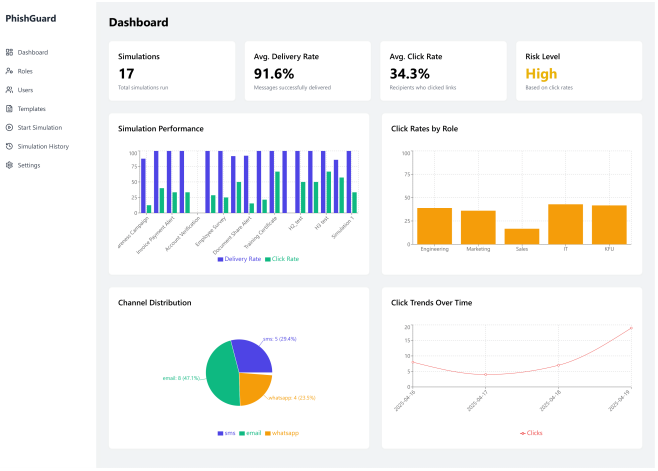

Fig. 9. Phishing simulation admin dashboard.

- Template Engine: Enables dynamic placeholder injection such as {{user_name}}, {{tracking_url}} and {{random_number}} which leaves room for maximizing personalization. Fig. 10 shows an example from the system.

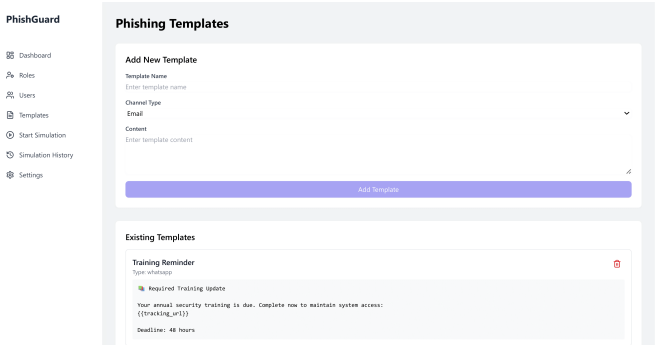

Fig. 10. Phishing simulation adding template page.

- Simulation Dispatcher: It sends out phishing messages through integrated Email, SMS, and WhatsApp APIs. Fig. 11 shows the interface of creating a new simulation, and this gets triggered after clicking the button.
- Tracking Mechanism: Unique tracking links record the user clicks, the timestamps, and response metrics. Fig. 12 shows the email received from the system after the launching of the simulation.
- Awareness Module: Immediately trains users who fall for simulations by redirecting them to an awareness page as shown in Fig. 13.

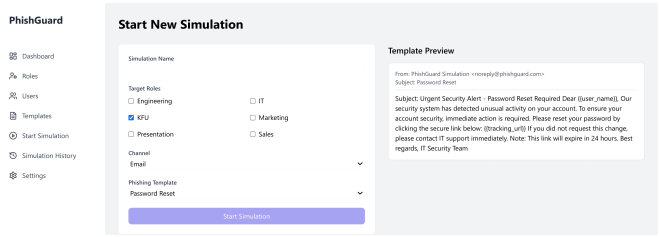

Fig. 11. Configuration setting of the simulation campaign.

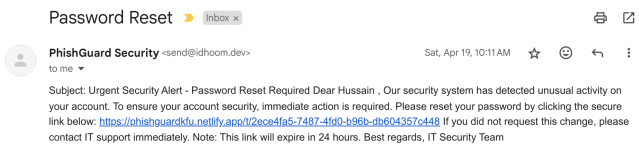

Fig. 12. Phishing simulation email received with a unique tracking link.

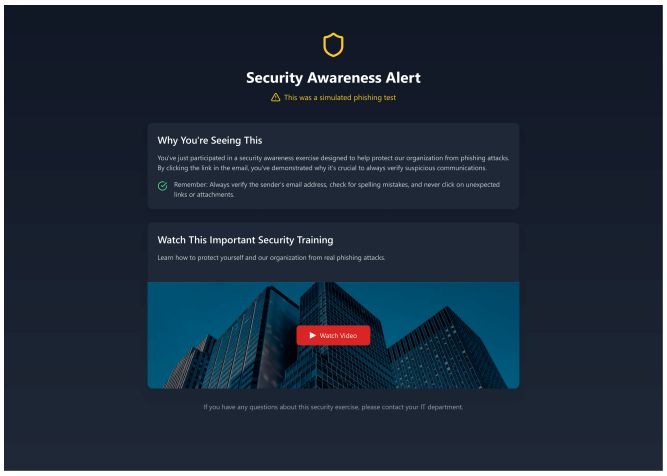

Fig. 13. The awareness page from the system.

- Database Integration: It normalizes the storage of all simulation data, logs, and user profiles.

C. Testing and Verification

To verify, individual core modules were tested.

- Correct rendering and substitution of template placeholders.
- A reliable way of interacting with an API for message delivery.
- Make sure accurate tracking of click events and response time.
- User interface that is responsive and compatible with browsers Chrome, Firefox, and Edge.

D. Deployment

The platform was deployed using Netlify, a cloud service platform that is known for being simple and powerful when deploying web applications. Finally, Netlify was used to host frontend components (admin dashboard and awareness pages), as they allowed for really fast, continuous deployment. This approach made for easy updates and a reliable way to host the web interface.

This section contains data and visuals generated from sample values to show the capabilities of the system. No real user interaction was recorded.

E. Behavioral Analytics and Reporting

The phishing simulation platform also includes a set of in-depth analytics that allows administrators to measure user behavior, campaign performance, and phishing awareness in terms of users, roles, and communication channels. The collection of data happens in real-time and creates an intuitive dashboard to visualize the data.

1) Admin dashboard reports: The key visual and statistical insights are available on the admin dashboard, which are:

- Total number of simulations conducted.
- The average delivery and click-through rates for each Simulation campaign.
- Low, Medium, High risk classification levels.
- Email, SMS, WhatsApp channel usage summary.
- Click trends over time.
- Click rate by role.

These visualizations that are shown before in Fig. 9 enable organizations to discover vulnerable users, assess the efficiency of training campaigns, and decide on the follow-up intervention.

2) Simulation history and detailed reports: All of the simulations executed within the platform are maintained on a complete history, which administrators can view:

- Simulation campaign names and associated templates.
- The targeted roles.
- Delivery rate and click rate performance.
- Channel of communication type used.
- Date and time of execution.

Fig. 14 shows lists of past simulation campaigns with delivery and engagement metrics across targeted roles.

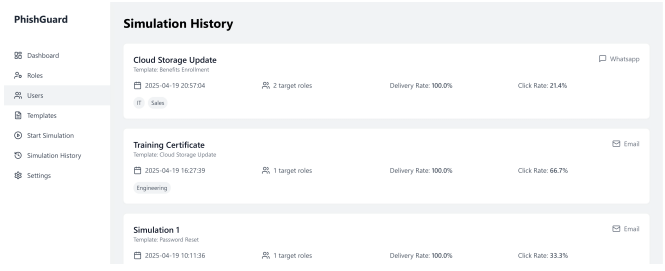

Fig. 14. Simulation history log – sample data.

By selecting a simulation campaign, you can discover detailed analytics and view these analytics:

- Date and time of execution of the simulation.
- Number of targeted roles.
- Delivery rate and click rate performance of the simulation campaign.
- The click rate per role as a bar chart.
- Overall response to the phishing message by click.
- List of users tragedy respect to user role along with delivery Status, click Status and the response date and time.

Fig. 15 shows an individual simulation campaign with its information and analytics.

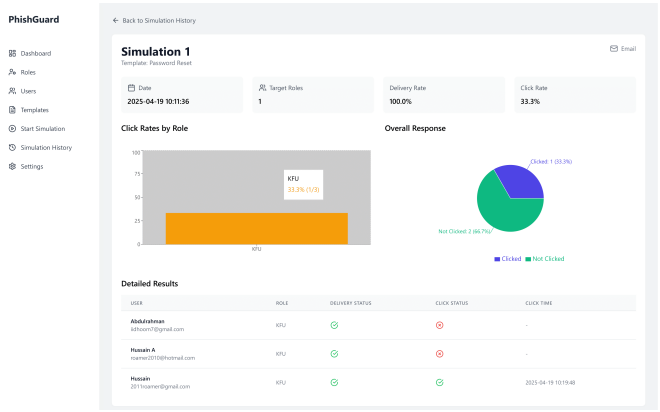

Fig. 15. Specific simulation campaign - analysis – sample data.

VI. Discussion

As a result, in this study, a customizable phishing simulation platform was presented for the improvement of user-specific cybersecurity awareness by means of targeted phishing and real-time behavioral analytics through multi-channel delivery. The proposed approach improves the traditional awareness methods by providing personalized simulations of the attacks through Email, SMS, and WhatsApp, which are a real attack vector. It generates phishing content dynamically using placeholders such as {{user_name}} and {{tracking_url}}, increases the user's engagement and offers an authentic environment to recognize phishing in familiar scenarios. Also, the behavioral tracking engine assists organizations in identifying click patterns and response times and identifies high-risk individuals with whom training intervention data can be linked. Furthermore, this also provides immediately awareness feedback to support just in time learning to reinforce safe practices when the users are the most vulnerable. Being adaptable, realistic and insightful at the user level, this directly fills the gaps in current generic, one-size-fits-all, one size fits all training programmes. Moreover, the system is deployed using a cloud-ready frontend with Netlify and has a modularity in the architecture that would make it a good candidate for real-world product adoption in enterprise environments where ongoing, customized phishing awareness is needed.

RQ1-RQ5 were created to serve as the system development framework and future evaluation. This paper is focused on the design, architecture, and demonstration of the platform through computational simulation. The above specifies the way each of the questions is answered at this step:

- RQ1 (long-term awareness and behavioral change): The proposed platform has modules of behavioral-tracking (e.g., click behavior, response time), which are proposed as a precondition to assess the long-term awareness and the following behavioral change of users.
- RQ2 (emerging behavioral patterns): The behavioral data produced on the platform enables a researcher to record the user response patterns based on the role and channel. These patterns provide a basis where emergent trends of behavior are identified.
- RQ3 (advantages of customization): The current platform enables the customization of simulations by the role and behavior of the user, unlike the standard, non customized training environment.
- RQ4 (engagement across platforms): Support multi-channel, but the study has not explored the differences between engagement across the channels.
- R5: (real-time feedback and analytics): The current platform delivers real-time awareness pages upon phishing link, but the study has not address the effectiveness and consider as future work.

The discussion in the current paper provides that the platform in question is intentionally designed in such a way that it can address the technical concerns identified, but its general effectiveness has not been tested and consider as future work.

VII. Challenges to the Study

Several challenges were faced in developing the phishing simulation platform. However, because of ethical restrictions, the system was not tested with real users, and all behavioral data were simulated inputs that restricted the ability to measure training effectiveness on real users. The platform was developed to support multi-channel delivery through Email, SMS, and WhatsApp, however, it was not possible to see how users might react differently on these platforms. Furthermore, the awareness page that is opened when a phishing link is clicked is also created with basic informational content and does not yet have interactive features like quizzes or scenario training. These improvements are slated for future versions in order to drive warmer engagement and better learning outcomes. In addition, there is no public dataset found that contains phishing simulation analytics or user behavioral responses with which to benchmark the system outputs against real-world baselines.

VIII. Conclusions

In this study, we design and implement a customizable phishing simulation platform to tackle challenges associated with traditional cybersecurity awareness training. From a review of the existing literature and tools, the research gap was identified that most of the awareness programs are

generic, limited to email simulation, not personalized, and do not provide real-time behavioral insights. The proposed platform then comes up with the multi-channel simulation delivery via Email, SMS, and WhatsApp, role-specific targeting, and dynamic template generation using placeholders such as {{user_name}} and {{tracking_url}}. All of these features make the simulation more realistic and engaging to the user. A behavioral tracking engine is also integrated within the system to track user interactions, assess risk levels, and provide immediate feedback via an awareness page, thus supporting just-in-time learning. The platform provides an administrator dashboard to analyze in detail campaign performance as well as user behavior for a given campaign and help to make the platform adaptable to a particular organization's needs. Due to ethical restrictions, the platform was tested with simulated data. Nevertheless, a cloud-ready frontend was deployed, and the platform shows potential for real-world use. Future work will be to conduct live evaluations, to enhance the awareness content with interactivity learning, and to complete integration of all communication channels for full multi-platform simulation capability.

FUNDING

This work was funded by King Faisal University, Saudi Arabia. [Project No. GRANT KFU252300].

ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT KFU252300].

CONFLICTS OF INTEREST

All authors declare no conflict of interest.

REFERENCES

[1] H. Shahbaznezhad, F. Kolini, and M. Rashidirad, "Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter?" *Journal of Computer Information Systems*, vol. 61, no. 6, pp. 539–550, 2021.

[2] U. Divakarla and K. Chandrasekaran, "Predicting phishing emails and websites to fight cybersecurity threats using machine learning algorithms," in *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*. IEEE, 2023, pp. 1–10.

[3] M. Rader and S. Rahman, "Exploring historical and emerging phishing techniques and mitigating the associated security risks," *arXiv preprint arXiv:1512.00082*, 2015.

[4] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers & Security*, vol. 132, p. 103387, 2023.

[5] M. L. Jensen, R. T. Wright, A. Durcikova, and S. Karumbaiah, "Improving phishing reporting using security gamification," *Journal of Management Information Systems*, vol. 39, no. 3, pp. 793–823, 2022.

[6] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, vol. 16, no. 4, pp. 527–565, 2022.

[7] S. G. Abbas, I. Vaccari, F. Hussain, S. Zahid, U. U. Fayyaz, G. A. Shah, T. Bakhshi, and E. Cambiaso, "Identifying and mitigating phishing attack threats in iot use cases using a threat modelling approach," *Sensors*, vol. 21, no. 14, p. 4816, 2021.

[8] C. K. Olivo, A. O. Santin, and L. S. Oliveira, "Obtaining the threat model for e-mail phishing," *Applied soft computing*, vol. 13, no. 12, pp. 4841–4848, 2013.

[9] M. A. Bawazir, M. Mahmud, N. N. A. Molok, and J. Ibrahim, "Persuasive technology for improving information security awareness and behavior: literature review," in *2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*. IEEE, 2016, pp. 228–233.

[10] P. K. Yeng, B. Yang, M. A. Fauzi, and P. Nimbe, "A framework for exploring incentive methods towards reducing phishing susceptibility in healthcare: Based on a review and in-the-wild-field study approach," *2023 Intelligent Methods, Systems, and Applications (IMSA)*, pp. 228–234, 2023.

[11] T. Sutter, A. S. Bozkir, B. Gehring, and P. Berlich, "Avoiding the hook: influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception," *Ieee Access*, vol. 10, pp. 100 540–100 565, 2022.

[12] B. M. Ahmad, S. M. Ahmed, and D. E. Sylvanus, "Enhancing phishing awareness strategy through embedded learning tools: a simulation approach," *Archives of Advanced Engineering Science*, pp. 1–14, 2023.

[13] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, and S. Furnell, "Evaluation of contextual and game-based training for phishing detection," *Future Internet*, vol. 14, no. 4, p. 104, 2022.

[14] S. Chatchalermpun and T. Daengsi, "Improving cybersecurity awareness using phishing attack simulation," in *IOP Conference Series: Materials Science and Engineering*, vol. 1088, no. 1. IOP Publishing, 2021, p. 012015.

[15] M. Canham, C. Posey, and M. Constantino, "Phish derby: Shoring the human shield through gamified phishing attacks," in *Frontiers in Education*, vol. 6. Frontiers Media SA, 2022, p. 807277.

[16] C. O. Tinubu, O. J. Falana, E. O. Oluwumi, A. S. Sodiya, and S. A. Rufai, "Phishgem: a mobile game-based learning for phishing awareness," *Journal of Cyber Security Technology*, vol. 7, no. 3, pp. 134–153, 2023.

[17] W. Yeoh, H. Huang, W.-S. Lee, F. Al Jafari, and R. Mansson, "Simulated phishing attack and embedded training campaign," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 802–821, 2022.

[18] A. Ciupe and B. Orza, "Reinforcing cybersecurity awareness through simulated phishing attacks: Findings from an hei case study," in *2024 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2024, pp. 1–4.

[19] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, and L. Coventry, "Phishing simulation exercise in a large hospital: A case study," *Digital Health*, vol. 8, p. 20552076221081716, 2022.