An Advanced Email Phishing Simulation Tool

by

Raksha Ravindra Deshpande

A report submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Cyber Security

Program of Study Committee:
Joseph Zambreno, Major Professor

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this report. The Graduate College will ensure this report is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2025

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

ACKNOWLEDGMENTS

I would like to take this opportunity to express my gratitude to my parents for believing in me and being a constant source of motivation, confidence, and a positive environment throughout my academic journey and life. I also thank Professor Joseph Zambreno for his constant guidance, patience, and support throughout this research and my project.

ABSTRACT

Despite advances in security technology, phishing continues to take advantage of human susceptibility, resulting in compromised confidential information, money theft, and damage to confidence. This paper discusses the design and development of a phishing simulation and behavioral analysis tool to improves in universities and organizational contexts. The tool utilizes Gophish to generate realistic phishing scenarios, Mailtrap as a secure SMTP relay, and Hotjar to observe individual user interactions with the phishing landing pages in real-time. This approach is unique in that, unlike traditional or existing phishing simulation tools, this tool adds to the effort of behavioral analysis, which in this case recorded all user interactions on the phishing landing pages, including cursor movement, interaction with forms, and click progression, so patterns in decision-making could be evaluated. All behavior and data analysis will serve as both an evaluator and demonstrate to what extent a subject was at risk of being compromised in phishing attacks, as well as feedback for subjects and suggested training. One of the most substantial contributions of this work is engaging heatmap-based analysis, and post-simulation awareness efforts help users to understand what their actions were and what led them to make those actions, taking into account their level of cognitive understanding. By implementing this approach of observation and feedback, passive training sessions created and used to train become an interactive and visual learning opportunity for a more in-depth understanding of phishing and improved retention. The results show a measurable substantial increase in the hesitancy among users even weeks after post-simulation, which aligns with the proposed tool. This process will provide the universities with a useful and deployable bridge between education and awareness.

CHAPTER 1. INTRODUCTION

Phishing is still one of the most ubiquitous and rapidly evolving threats in cybersecurity, impacting individuals and organizations around the world. While traditional threats operate exclusively through technical vulnerabilities, phishing threats prey upon human behavior, making them difficult to protect against through ordinary security measures. While firewalls, spam filters, and awareness training have greatly improved, phishing continues to flourish based on manipulating users through social engineering into revealing sensitive information. This project is focused on addressing this challenge using a simulated phishing attack and behavioral analysis tool that extends beyond standard phishing testing. With the tool, users will not only experience a realistic phishing attack using simulated emails and login portals, but will also have their behavior analyzed and monitored in real time. To do that with behavioral measurements, key indicators like click behavior, hover behavior, form behavior, and response time are collected with the help of Hotjar to gain additional insights into users' decision-making when immediately confronted with potential danger. One key contribution is the real-time behavioral analyses used for personalized adaptive awareness. Users will understand their performance feedback, but will actually see their clicks, hovers, and impulsive actions in the task. The feedback will be visualized with the support of heatmaps and interaction data, which will enhance retention and learning. The simulation environment utilizes Gophish and Mailtrap on a secure DigitalOcean VPS, rendering the project ethical and controlled testing. The architecture supports departmental-level risk profiling and offers a comprehensive supporting framework for broader organization awareness programs. By transferring to a simulation and utilizing progressive views from a dashboard, this project merges simulation, real-time tracking, and customized training that creates a feedback loop that actively boosts user resilience. The objective is not only to measure user awareness, but also to improve metered user awareness through awareness training. The

proposed approach provides answers to gaps identified in current phishing training solutions that mainly report on click-through rates, but do not identify why users are victimized by phishing in an actionable manner to improve their behavior. Additionally, this research adds a scalable, interactive, and user-centric, to the subject matter of phishing prevention to universities and organizational cybersecurity education.

CHAPTER 2. RELATED WORK

Research into phishing has shifted from a primarily technical analysis perspective to a more complex social/psychological perspective. A number of studies have noted that human decision-making, as opposed to just technology, plays a significant role in the willingness to engage in phishing. This influence has shaped the direction of simulation and behavior tracking developments, on which this project is built.

2.1 User Behavior and Psychological

The authors in [1] talk about the study that collected behavioral data that included click-to-read patterns, and to examine how users process phishing cues, the duration of each mail was recorded. The paper indicates that minor behavioral traits contribute to susceptibility. The study captures multiple points on how to advocate for behavior-aware training methods. The research encourages a psychological understanding of an employee's behavior in relation to preventing phishing. Expanding on the behavioral insights, this study [2] here concentrates on recognizing individual perceptions during email evaluation and serves as the foundation of PEST, which researchers use to gauge user suspicion levels at their detection-based facilities. The framework standardizes phishing detection tasks because it helps identify cognitive elements that affect decision-making processes. User suspicion levels differ according to how tasks are designed and the structure of email content. The application provides standardized assessment capabilities that support environmental and population-based comparison. The tool operates as a diagnostic system that helps evaluate and upgrade training programs. Continuing the focus on user behavior, another research [3] demonstrates that both fear and urgency play essential roles when attackers succeed in phishing attacks. The study investigates the process through which emotions invalidate rational decision-making abilities in users. The author suggests emotional profiling as a

developed defensive procedure. Training initiatives should be developed according to individual emotional needs. Phishing prevention requires psychological resilience, according to this research. Building upon the emotional and psychological dimensions, further researchers studied through this [4] how personality traits influence individuals' tendency to fall victim to phishing attacks. The research uses authentic phishing simulations to demonstrate how extroverted people, along with open-minded individuals, are most likely to fall for this type of cyber threat. Traditional training methods seem less impactful for particular personality types according to the research findings. Personalized interventions need to use psychological profiles to make effective interventions. This work expands human-element knowledge within the cybersecurity field. Reinforcing the importance of real-world behavior analysis, the research [5] shows that behavior patterns, including hesitation and confidence issues, together with blind faith in others, produce specific outcomes. The observed behavioral patterns help develop training platforms that imitate actual security risks. Security awareness training modules should incorporate behavioral assessment features according to research findings. The research offers a workable connection between defensive technology and psychological research practice. Adding to this, the paper [6] talks about how Phishing susceptibility is affected by both individual traits, including age, impulsiveness, and email behavior patterns. Research findings identify mail processing behavior as the most important predictor factor. Research suggests individual training programs should be developed from these identified characteristics. The paper demonstrates the advantage of adding behavioral profiling to security management systems.

The research identifies that people exhibit different levels of vulnerability to phishing attacks. To further structure user risk prediction, a model [7]evaluates phishing success rates through user behavior analyzed in three stages, which start with exposure and continue with engagement before submission. The sequences move according to mental and psychological components throughout. Knowledge gained through the funnel model enables the interruption of phishing attempts. Predictive defense strategies receive support through this model framework. Through this model, organizations obtain data for predicting risk levels that vary across different

user milestones. Extending phishing analysis beyond email, the research [8] explores how phishing has increased through messaging platforms as its main topic. The research establishes a connection between user self-confidence and privacy perspective with their vulnerability exposure. People who demonstrate higher levels of confidence, along with awareness, tend to lower their exposure to risks. The proposed research suggests providing specific educational programs for messaging platforms that receive heavy use. This paper extends phishing research boundaries by moving past email investigations. Turning attention to user interactions with interfaces, another study [9] examines the behavior of users when interacting with phishing emails and fake websites. The research has demonstrated that users do not often, if ever, verify the URL before disclosing information, and do not recognize soft cues. User behavior levels of digital literacy strongly correlate with their phishing email interactions. The authors support design improvements that are user-centric in web browsers and email platforms, but note that user behavior should be treated separately when designing awareness modules. Strengthening the case for personalized training, the research [10] talks about how it connects personal actions with phishing susceptibility through the examples of link clickers and email detail readers. The system helps organizations detect user behavior patterns suitable for focus in training efforts. According to the study, both vulnerability and diagnostic evaluation are based on behavior. The proposed strategy involves tracking user actions and using training practices that relate to the provided performance feedback. The system facilitates identifying user profiles to build awareness solutions with individualized approaches. Finally, to enable more proactive protection, a model [11] that predicts phishing susceptibility uses attributes from behavioral patterns with demographic indicators and environmental variables. The prediction model relies on three fundamental factors, which are age, browsing activities, and the records of email interactions. The predictive model achieves both strong accuracy results and applicable usage in practical settings. The method allows professionals to take preventive measures with users who are at elevated risk. The system allows personalized data-based training combined with individual monitoring solutions.

2.2 Detection and Prevention Techniques

The authors of the paper [12] look at how visual cues, such as the use of color codes and warning labels, help users when detecting phishing emails. In an eye-tracking study, we find that users who look at risk indicators become better at detecting phishing emails. The empirical findings across this study demonstrate that visual design has a real impact on users' decision-making. This study demonstrated that suitable changes to the interface could significantly impact user's ability to detect a phishing email. The authors suggest that introducing risk aligns, indicators, or even color coding into email or email platforms will provide more information for users to be able to manage the risks when opening emails. Building on visual design implementation, the proposed framework [13] uses AI technology by merging ML algorithms alongside behavioral symptoms for performing dynamic phishing attack detection. The model evolves through its analysis of current user actions, including mouse tracking and click behavior. Such a filtering system demonstrates more accurate results, together with faster detection rates when compared to older static filtering solutions. Enterprise incident detection gains enhancement through the implementation of this hybrid approach. The system introduces a new direction toward security measures that receive and respond to user behaviors autonomously. In support of more accurate detection models, the research [14] focuses on essential behavioral features aimed at improving detection algorithms. A process of engineering features will assist with better performance in classification systems. The enhanced feature refinement methods provide results that are accurate and with decreased noise levels according to the study's findings. This research development leads to better phishing detection systems. Experts agree that feature selection is the first and most important step in model creation. Expanding the scope to the blockchain environment, the research [15] shows how it investigates Ethereum transaction phishing activities through systematic time patterns and structural indication evaluation.

A particular series of steps, combined with time delays, functions as a signal to indicate deceptive transactions. Security alert systems develop their functionality using these observed

behavioral cues. A new defensive strategy against phishing attacks in cryptocurrency platforms represents the main contribution of this study. The research holds importance for blockchain adoption because of the increasing security threats in this space. To understand phishing from both a technical and psychological way, another study [16] examines a widespread phishing attack to identify its psychological manipulation techniques along with the technical exploitation methods. The study reveals success elements, which include urgent requests for established authority and tailor-made deception methods. The research about attacker strategies enables organizations to create multiple defense layers. Technical solutions cannot establish security on their own because they need additional support. For effective defense protection, users must be trained, and filtering methods must function with a strategy. Looking at the phishing incidents, the research [17] investigation explores what happens to user behavior after initial phishing experiences. Some users gain better caution, while others experience a reduction in their sensitivity. After attacks, the education system must operate to strengthen user awareness levels. The paper focuses on incident-based learning. The proposed method for defense involves behavioral reinforcement. Finally, a broader view is presented in the study [18] shows the authors compared different detection methods for phishing by blacklists, heuristics and machine learning-based models. This paper discusses the advantages and disadvantages of each method that was selected. The paper shows how detection speed and collisions with detection accuracy are associate with the detected false positives. The paper provides a comprehensive resource for users to assist with method selections. The work illustrates the need for an array of security protection mechanisms.

2.3 Experimental Design and Methodology

The author of the paper [19] discusses the research problems for researchers who undertake phishing experiments. The problems are of a conflict, which include ethical issues, technical, and operational concerns. The authors stated that finding responsible user consent was an important conflicted concept that was not a limitation to the validity of the study, but not all other research

problems were creating a simulated phishing experience that was genuine while protecting the ethical and legal position as a researcher. The authors then advocated for a style of framework for the researcher and demonstrated elements of what it takes to create ethical research question papers. The authors also argued in favor of adopting the practice to disclose or practice open reporting of research methods and safety protections for participants. This study helped to generate effective ethical research on phishing. Extending the discussion into practical experimentation, the [20] research examines the response of students and academic staff members to assess their susceptibility to phishing attempts. Most participants missed the phishing elements in the simulation, while students displayed increased susceptibility to phishing attempts. The research established that institutional training programs and awareness sessions do not provide adequate learner outcomes. The paper provides specific recommendations that educational organizations can use to decrease their exposure to risks. Academic institutions require proactive security measures to develop within their environment, according to this research. Further exploring experimental setups, the [21] research analysis the effects of using time countdowns combined with pressure-indicating cues on user behavior. Time limits in research data prove that they lead more users to select dangerous website links. Empty or busy scenarios let cybercriminals outrun target evaluation processes. As part of their program, training should include simulated urgent conditions to develop resistance in users. This research paper establishes urgency as a mental attack mechanism that works through intimidation. To complement these experimental approaches, the [7] model analyzes three stages, which are exposure, engagement, and submission by users, to forecast the outcomes of phishing attacks. Every stage within the model depends on both emotions and thinking factors. The funnel structure presents data that helps to find opportunities for stopping phishing attacks. Predictive defense strategies find support from this model. Through this model, organizations obtain insight about risk levels that users encounter at various points in their activities. Shifting focus to cognitive modeling, the study [22] analysis integrates research results about phishing education through multiple studies. The analysis finds three main problems within training systems,

including excessively repetitive programs, insufficient customization, and variable results. The key elements supporting success comprise design, along with real-world simulation and repetition. This paper provides an outline for creating efficient phishing training programs. Education under this method promotes ongoing adaptive teaching strategies that follow behavior changes.

In line with cognitive-based approaches develops a computational model [23] is developed that analyzes user behavior when they determine whether emails are phishing communications or not. The model analyzes quick thinking methods together with judgment errors found in decision processes. The model discerns patterns in wrong decisions. The collected results will be beneficial for training development, along with user interface improvement projects. The model connects aspects of cognition with cybersecurity disciplines. Continuing the investigation into human-centered security, this paper [24] presents different findings about emotional patterns, cognitive processes, and behavioral elements in phishing attacks. The system classifies human weaknesses into distinctive psychological behavior patterns. The data reveals that human mistake leads to phishing attacks that end up successful. The analysis recommends that technical solutions must join forces with psychological theories to solve phishing vulnerabilities. Future studies on human-centered phishing research will use this review as their starting point. Adding further experimental perspective, through experimentation [25], the role of user mistakes with system design problems in achieving phishing goals is evaluated. Users make additional errors when interfaces are poorly designed, according to this research. Human effort is insufficient to protect against phishing attacks unless backed by proper systems. The article promotes the integration of usability with training measures. It supports human-centered security design. Finally, moving toward technological advancements, the investigation [26] analyzes how LLMs, including GPT, can identify phishing content. The models presented hopeful results, but researchers noticed problems with incorrect positive results along with limited knowledge of textual context. The research shows the strengths, together with the boundaries of AI systems in phishing protection. The paper suggests LLMs should operate together with human analysts and rule-based systems. Such mixed detection systems produce superior threat recognition outcomes.

2.4 Training and Awareness

This section concentrates on the area of how dashboards are utilized to keep track of phishing simulations. The author in this paper [27] highlights what percentage of employees were affected by phishing attempts, which provides real-time feedback on user behavior. The data-driven approach identifies vulnerable populations in support of training options that can be designed to target specific groups. The dashboard provides a way for organizations to illustrate engagement and facilitate adapting awareness methods. It bridges the data from user behavior analysis and security-awareness education. This investigation reminds the reader of the impact user behavior has on susceptibility to a phishing attack in relation to email reading behavior. Building on the need for more interactive and participatory approaches. A mixed-design [28] experiment indicates that collaborative techniques such as group discussions and role-playing show greater improvement in phishing recognition than academic instruction. These same collaborative techniques also produced greater self-efficacy and reporting. Users also had better retention and engagement one month later. The findings lend support to the theory of translating passive learning into our models of active participation. It is also indicated that providing interactive training is a significantly more effective awareness strategy. Continuing the examination of training methodologies, the researcher [29] found that scenario-based training was the best approach overall. The researcher emphasized the significance of reinforcement training, provided that it must also be personalized and delivered. The research concluded that there is no best method because there must be contextual training, but there is a lot of good information to help program designers. Turning to user interface and automated support, the research [30] demonstrates that gentle warning methods decrease user's risky choices substantially. The tools demonstrate varying results depending on the user category. The authors recommend adopting adaptive instruments that modify their responses based on user patterns. The integration of advanced interface functions is part of blocking phishing attacks.

2.5 Gaps Addressed by This Project

While prior research has duly recognized the need to study psychological traits and behavior, few studies have integrated a phishing simulation, behavioral analysis, and personalized feedback in one system. Although many tools allow tracking the event of a user clicked a link (generally labeled as clicking a phishing link) very few study the user's behavior thereafter. This project directly addresses these gaps: Real-time tracking of scrolling behaviors (e.g., cursor movement, scroll depth), Visual feedback to users via heatmaps. Risk-based user categorization and targeted training. In this way, the project improves an interactive, data-driven phishing awareness that focuses on registered user's actual behaviors. As such, it adds a novel contribution to the research and practice of phishing prevention.

CHAPTER 3. METHODOLOGY

The chapter explains in detail the systematic development and evaluation process of an advanced phishing email simulation coupled with a behavioral analytics system. The methodology merges realistic simulation techniques of phishing attacks with user engagement tracking, along with risk identification abilities and unique training solutions for particular vulnerability areas, into a single system. A secure ethical process conducts these elements to provide participants with a protected educational environment, which boosts their cybersecurity readiness.

3.1 Research Question

The research provides an answer to a targeted practical problem by investigating "How do we track and analyze user behavior in phishing attacks to use tailored feedback which improves cybersecurity awareness?"

The research focuses on real-time user analysis of interactions instead of conventional phishing threat detection methods and generalized user training programs adopted in previous studies. My research analyzes the psychological weaknesses of people looking at possible phishing activity to reveal attack entry points.

The research seeks to develop behavioral feedback analytics, which will become an important tool for obtaining user data. The focus of this method targets user-specific requirements to teach people about phishing threats and support better cybersecurity practices. I aim to develop specific feedback methods to build a more active and aware user community that notices emerging cyber threats.

3.2 Research Approach

This methodology employs a multifaceted experimental and user-centered approach, which consists of several sequenced detail steps to summarize the state of the research and understand better how actual human subjects respond to phishing attacks.

1. Controlled Phish Simulations: I used our sophisticated phish occurs designed by emailing simulated actual campaigns and deceptive web pages. I designed these simulations to appear as actual phishing attacks, and they work exceptionally well in obtaining user awareness and response.

2. User Behavior Tracking: I used high-level analytics to track user behavior during the phishing simulations. This includes tracking click-through rates on links, the amount of time spent on pages, and overall engagement. This information allows us to make observations about how users are interacting (or engaging) with simulated phishing attacks.

3. User Classification: Analyzing the results in relation to engagement with videos and tracking responses gave me a level of user classification about successful phishing attacks or loss of phishing resistance. Therefore, I begin to look for clues to statistically classify user likelihood towards phishing engagements (e.g., similar user responses to the simulated attacks) with higher levels becoming profiles of users that suggest likelihood based on the user engagement responses relation to phishing engagement.

4. Feedback Creation and Training: Upon completion of the simulations, I will generate a feedback report for the participant showing where they demonstrated who was resilient to phishing risk. Based on this information, looking at and suggesting deeper engagement to strengthen phishing resistance and resilience to probable phishing attacks.

3.3 Limitations of the Methodology

The research methods for this project describe a new and innovative combination of real-time behavioral analysis and phishing simulations; however, it is worth noting the limitations that would influence the extent to which the results are generalizable to other settings and scalable to other populations.

1. Small User Sample: The phishing simulations were executed in a controlled environment and, therefore, with a modest number of users. This would limit the type of user behavior observed in the simulations and generally not account for the breadth of responses of users found in most large organizations with various roles, experiences, and levels of awareness.

2. Limitations of Tool: Hotjar was utilized to track behavior, but was on a free-tier plan, and analytic sessions were constrained in their length or the number of sessions captured. These limitations may have biased or diminished the resolution of the user interaction data, limiting what could be learned in the analytics and interpretation of details related to behavior patterns.

3. Simulated Context vs. Actual Behavior: Users had the knowledge they were participating in some testing environment, regardless of whether they knew what the simulation was specifically convened for. This knowledge might change behavior in ways that lead users to be more conservative than they would be in real-world scenarios. Therefore, results may not perfectly reflect actual vulnerability to real-world, genuine phishing attacks. Ultimately, these limitations notwithstanding, the method offers a good starting foundation for future use, and these limitations can be sufficiently improved upon with iterative development, scaling deployments, and upgraded tools.

3.4 Data Analysis Techniques

Behavioral data from the simulations was examined using both **quantitative** and **qualitative** analysis to build a holistic view of user behavior.

1. Quantitative Analysis: Numerical metrics were determined to characterize user behavior patterns.

    - Click-through rates, time on page, and scroll depth were compiled to understand exposure to risk.
    - Frequency of interactions with specific elements on the page (e.g., login buttons) was obtained.
    - Charts were developed to visualize data and identify trends across user groups.

2. Qualitative Analysis is Each user's session was analyzed in detail. Heatmaps showed visual representations of clicking and attention zones. Recordings of cursor movements were manually reviewed in order to gauge the tendencies of users´ intent to decide. Actions such as hovering without clicking, random movements of the cursor were taken as potential indicators of users being uncertain of what to do or feeling too confident in their actions.

CHAPTER 4. EXPERIMENTAL DESIGN

During the setup phase, I got the infrastructure ready to conduct simulations, ensuring that it all works as one, with no risk to real users. This phase consists of both the tools I will be utilizing as well as configuring the phishing campaign environment.

4.1 Tools and Technologies

1. Gophish: Gophish is a freely available open-source phishing platform that serves the role of a simulation engine. It provides the features to create phishing campaigns, such as email templates, landing pages, and user tracking features. Links and behavior tracking are built into Gophish and can capture user behavior such as opens, clicks on links, and timestamps, which makes it appropriate for behavior experiments.

2. Mailtrap is a simulation SMTP server to guarantee secure messaging routes for all simulated phishing emails among protected simulation environments. Mailtrap constitutes a unique SMTP server because its test messaging function prevents unintended email delivery to real users, which protects both simulation ethics along recipient privacy boundaries.

3. Hotjar: Hotjar provides live behavior analytics of phishing landing pages. Hotjar captures and tracks user's mouse movement, clicking patterns, scroll depth, and time spent on a phishing page once the users arrive on the page. This data is reflected back to the researcher in the form of behavior heatmaps or session recordings depicting the patterns of interaction.

4. The simulation operates on a secure Virtual Private Server, which DigitalOcean provides from their platform for users. Gophish and landing pages, along with analytics scripts, operate from a DigitalOcean VPS that ensures complete security by keeping them separate from user-related systems.

4.1.1 Setup Activities

1. Gophish Configuration: The Gophish software was installation onto a DigitalOcean VPS after connecting with Mailtrap for secure SMTP handling to monitor email delivery. The authorization screen for the dashboard required a password entry, while additional protection came from IP restriction policies.

2. Email Template Design: During the design phase for email templates, realistic methods were employed to represent how social engineering vulnerabilities would be exhibited in everyday applications. Gophish demonstrated emails by showing fake alerts for access to login and password expiration notifications. The users were directed to appropriate landing pages via custom-embedded links in each email.

3. Landing Page Creation: Every landing page received its own design meant to duplicate the appearance of the official business login portal. Tests were designed to replicate the usual activities, such as urgency for password update, together with layouts and button placement for a realistic simulation without compromising actual credential entry.

4. Hotjar Script Integration: Every landing page incorporated its own Hotjar tracking code, which the developers manually inserted into its source code through HTML. The controlled conditions allowed for tracking user activities in real time without seeking user permissions since the test environment informed participants about the monitoring procedures.

5 End-to-End Testing: The campaign received an end-to-end test as the final stage before its release. System testing involved sending emails while users clicked links, which produced behavior monitoring data to check every system component, starting from the delivery to heatmap generation. Proper attention was devoted to verifying that protected data remained secure and was prevented from transmission.

4.2 Execution Phase

The whole phishing simulation process originated from my work, where I controlled all parts of the campaign, starting with email composition, continuing with simulation deployment, and observing active user actions. During this phase, I achieved the technical endpoint while conducting controlled participation with test participants under ethical terms. Once the infrastructure setup completes, the execution phase routes the phishing simulation to its active deployment steps. I then conducted phish testing for users by monitoring their responses through email surveys, then recording complete operational data for evaluation purposes.

4.2.1 Email Campaign Launch

In my project, I deployed phishing campaigns through Gophish, which served as my design platform. I made professional email templates that reproduced regular phishing deceptive email styles, including notifications about passwords and security warnings. I focused on careful management of formatting techniques to make the emails look legitimate, along with proving their authenticity. The emails were sent to test accounts through a medium that notified participants about joining the protected simulation environment. Properly delivering secure emails required me to integrate Mailtrap as the SMTP service. All emails that passed through Gophish were configured with the credentials of Mailtrap, which maintained them inside a secure testing environment. The setup protected me from exposing unintended recipients because it allowed me to confirm email content and deliverability, and format without such exposure. I designed the campaign runs for regular working hours because I wanted to create genuine phishing situations. The guidelines provided by Gophish through open rates and link clicks enabled monitoring of user engagement with sent emails. The Gophish platform enabled me to generate attacker-simulated email messages that imitated standard field-based assault initiatives through password expiration alerts and security verification requests. The phishing attacks incorporated authentic company branding elements, together with reliable design elements from company emails, along with consistent sender details. The dummy accounts received the campaigns, while individuals from

selected groups received notification of testing following approval under ethical standards. Users who clicked on the tracked links were redirected to safe simulated pages that operated from secure DigitalOcean VPS servers. Mailtrap functioned as an SMTP server that protected email delivery safety when testing occurred in protected environments and prevented delivery to unintended recipients. The secure email sandbox offered by Mailtrap serves developers and testers through email interception, which makes it suitable for phishing simulation and development work. The scheduled email distribution happened during usual work hours to mimic real phishing scenarios appearing in normal operation hours. The Gophish system utilized Mailtrap's SMTP credentials, which allowed tracking of delivery status, combined with open rates and click-through behavior data for every recipient, thus enabling research into initial phishing engagement behavior.

4.2.2 User Interaction and Tracking

When users clicked phishing links contained in the emails, they were directed to secured landing pages that I hosted on DigitalOcean VPS. The fake login interfaces on these pages displayed appropriate elements to fool users, but they functioned only to track user behavior. Hotjar tracking code was implementation across every landing page to capture complete user interaction information. Users showed their cursor movements while they hovered above links and buttons, and indicated their behavior by scrolling down the page or leaving immediately. During my analysis, I reviewed the heatmaps while watching real-time session recordings because they showed user hesitation behaviors and decision-making as well as their engagement patterns. The recorded user behavior revealed caution or impulsivity that determined their risk type needed awareness training. Users who clicked the phishing link were redirected to the original website, and activities on the fake login pages were monitoring their interactions because of the included Hotjar script. When Hotjar triggered the page load, it started tracking how users operated their mice and the locations where they hovered, as well as each click and scroll depth. The real-time recordings enabled experts to assess user attention as well as hesitation and exploration, and

impulsivity. The interaction data formed the basis for creating user awareness as well as building unique training impacts.

4.2.3 Simulated Behavioral Scenarios

The evaluation revealed three primary ways users behaved during the survey session.

1. Slightly more than ten percent of users hit the login button or touched form fields instantly within the first second. Users who immediately clicked buttons in the form qualified as highly susceptible since they displayed zero safety precautions.

2. Other users demonstrated caution by allowing their mouse movements to explore areas of the page and by both hovering over items and gradually performing page scrolls. The observed conduct reflected users who displayed better cognitive abilities and higher awareness.

3. Users who departed from the page before taking any action showed they understood this attempt as a phishing incident. The users who took part displayed both high perception skills and minimal vulnerability to phishing attacks.

The experimental scenarios functioned as core elements in establishing user behaviors so trainers could create personalized performance evaluation feedback.

4.3 Data Collection Phase

After the phishing simulation finished, I started with data collection procedures. Evaluating simulation effectiveness and user behavior analysis required this step as its main component. My objective was to extract full data from Gophish and Hotjar, and Mailtrap to create awareness measurement training.

4.3.1 Data Sources

The behavioral and campaign data required multiple integrated tools for both collection and cross-referencing operations. The union of data collected from these three tools allowed me to create a comprehensive picture showing when users received emails through their activities on the landing page. Gophish provided campaign-level metrics including:

- The tool reported total email transmission and successful delivery along with email rejects.
- Open and click-through rates.
- Users took action after the delivery of email messages.

Hotjar captured page-level behavior including:

- Mouse tracking heatmaps.
- Session replays for individual users.
- The tools evaluated were Click maps used alongside a technology called Scroll depth analysis.
- Form engagement without submission.

The SMTP relay platform belonged to Mailtrap. All emails sent from the platform underwent delivery and storage as backup for testing and validation through Mailtrap. Through its platform, these emails remained separate from external servers, and the platform enabled header and content verification as well as delivery metrics checks. The gathered data provided both quantitative measures and qualitative data that could be used for the user awareness training analysis.

4.3.2 Data Structuring

When I had gathered the raw data from all sources, I began a formal analysis of the data. I analyzed the data and the behavior of the users.After analyzing the data, some of the common patterns that I found in users are as follows.

- Time spent on the landing page.
- Time of scroll behavior.
- Amount and direction of cursor movement.
- The number of clicks on interactive elements or entry fields.

Users were divided into three discrete risk categories:

1. **High Risk:** Users engaged in rapid click behavior without content exploration or engaged in impulsive interaction with form fields.
2. **Moderate Risk:** Users engaged in click behavior with hesitation and some level of exploration.
3. **Low Risk:** Users that had early drop-off behavior or cautious behavior such as hovering without clicking.

Once I had categorized this behavioral data, I used heatmaps, bar graphs, and timeline charts to represent this behavioral data and look for patterns. Using these visualizations, I was able to identify clusters of behavior, such as users who clicked too rapidly or users who physically never engaged at all.This structured data was critical for guiding personalized feedback and awareness materials.

CHAPTER 5. SIMULATION OUTPUTS

5.1 Godaddy domain name raksha.me

The creation of a realistic phishing simulation required me to use GoDaddy for managing and registering the raksha.me domain. The domain server enabled the creation of more authentic phishing messages and destination pages. Creating a domain with an authentic appearance became essential to achieve real-world simulation conditions by granting complete DNS and redirection management of my hosted Gophish platform. Figure 5.1 shows a screenshot of the domain registration for the raksha.me domain.

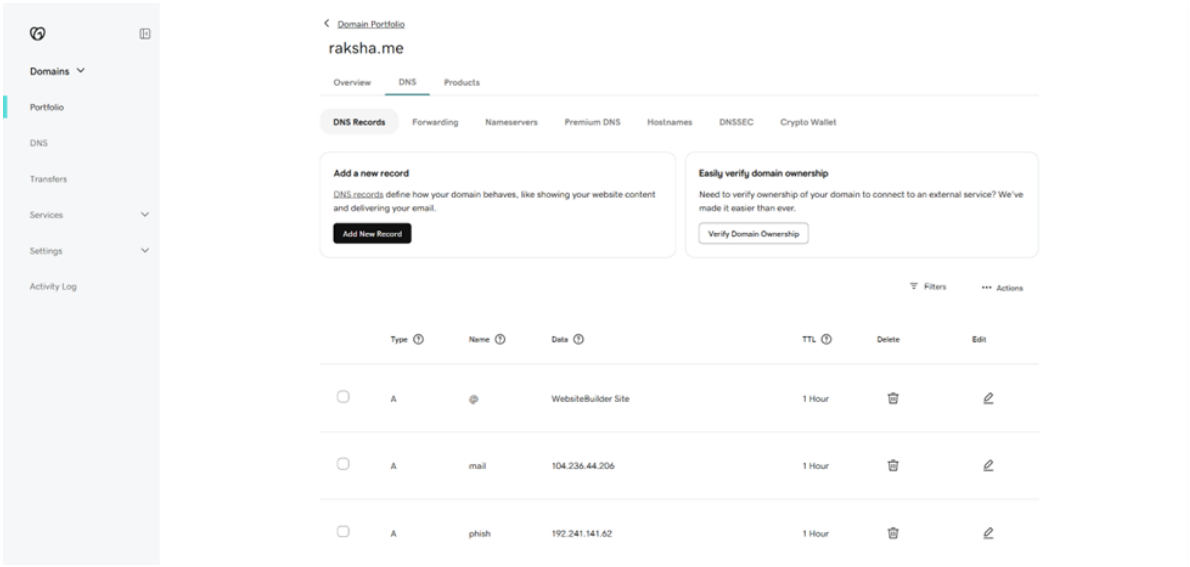

Figure 5.1 GoDaddy domain name raksha.me

5.2 Digital Ocean - VPS SERVER: Gophish Demo

I installed a VPS instance under the name “GOPHISH-DEMO” on DigitalOcean for secure simulation execution. Running Gophish on its own VPS server gave me full control to customize

campaigns and adjust SMTP configuration as well as monitor behavior statistics independently from third-party systems. The complete operating environment remained under controlled conditions in this setup. The image highlights my phishing simulation cloud provider. I used the Digital Ocean cloud host provider and hosted a Gophish-demo VPS Server instance. I used this server to deploy and manage the phishing campaigns. It is an isolated, ethical testing environment away from the real world. Figure 5.2 showcases the DigitalOcean: VPS server: Gophish-demo.

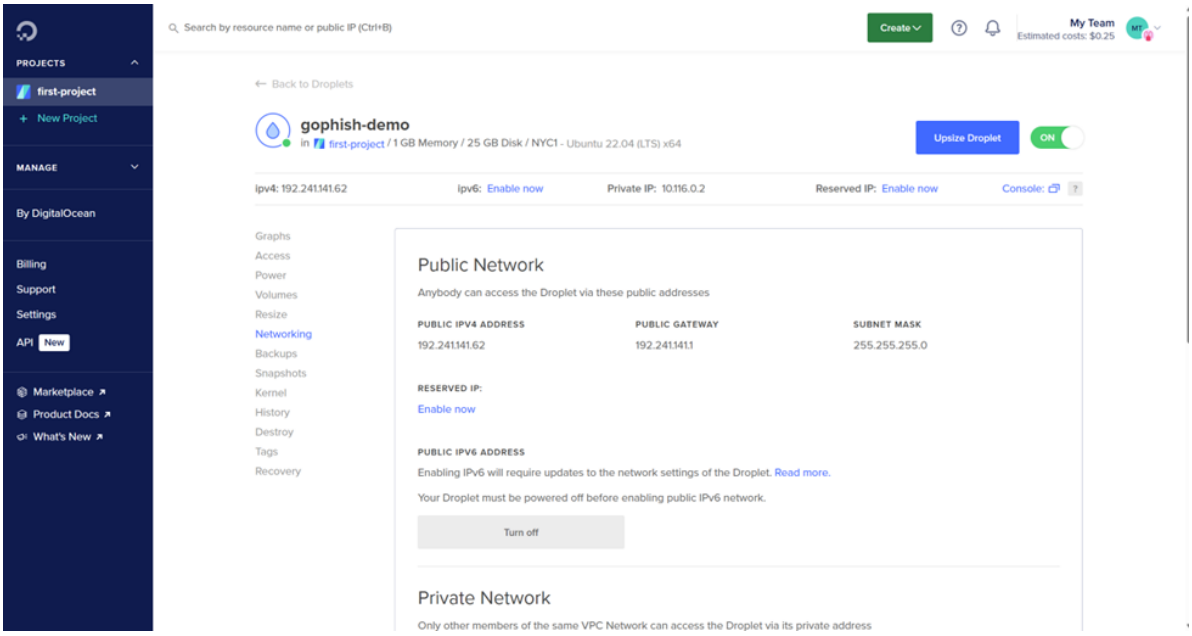

Figure 5.2 Digital Ocean - VPS SERVER: Gophish Demo

5.3 SSH-Gophish Connection

Through this snapshot, I successfully connected to the Gophish server over SSH, which granted me access to diverse, powerful features. I configured Gophish thoroughly under this access while skillfully adding attractive templates and tested the server's operational efficiency. Secure terminal access proved essential in the entire project because it let me easily execute backend updates and maintain a confident approach toward launch and troubleshooting campaigns.The Gophish site: https:phish.raksha.me:3333. Figure 5.3 showcases the logging into gophish. SSH into Gophish.

Figure 5.3 SSH-Gophish Connection

5.4 Gophish Login Page

The Gophish administrative dashboard required me to use this page for access so I could conduct strategic operations on my phishing simulations. Through this central interface I carefully executed different operational elements including detailed profile generation and email template development and landing page creation and performance metric inspection. Through this platform I directed all my experimental activities with both accuracy and analytical understanding. Figure 5.4 showcases the logging into gophish.

5.5 Phishing Campaign Simulation Result

The snapshot vividly captures the phishing campaign demonstration, meticulously tracking every detail of user interaction, from email opens to clicks on deceptive links. This assessment offers a clear view of how engaging and persuasive the simulated attack was, revealing its effectiveness in captivating user attention and highlighting the vulnerabilities in their online

Figure 5.4 Gophish Login Page

behavior. Figure 5.5 showcases the phishing campaign simulation result I conducted to monitor user behavior.

5.6 User Phished Data-Demo Campaign

In this image, the users submitted data on the fake login page, simulating a successful phishing attempt. This helped quantify how many users would have been compromised in a real-world scenario. Figure 5.6 showcases the user data that was phished during the simulation.

5.7 MAILTRAP SMTP: User Test Emails

In this image, I used mailtrap as my SMTP server to use and host test emails. It captured all outgoing emails, ensuring that simulations stayed within the test boundary. Emails were sent to all the dummy users. The email included urgency for sign in activity, and users were prompted to change and update their passwords. Figure 5.7 showcases Mailtrap, which I used to carry out the test emails for the phishing simulation.

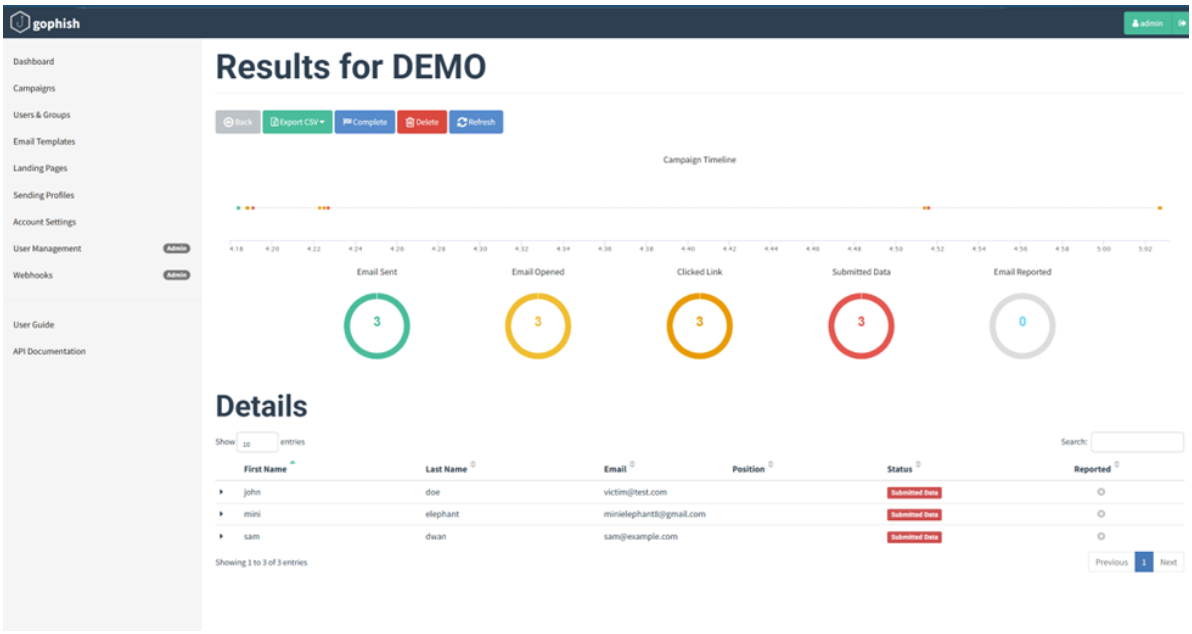

Figure 5.5 Phishing Campaign Simulation Result

5.8 Google-Fake Login Page

This image shows a convincing fake login page created to imitate Google's login portal. The fake login page, on entering the required details, redirects to the original Google login page. Figure 5.8 showcases the fake login page I interpreted for the phishing simulation.

5.9 Hotjar-Phished User Behavior Overview

This image displays the phished users overview on Hotjar. It shows a heatmap showing high-click activity areas, such as login buttons and links. The amount of time users spent on a page, average scroll depth on the page, and drop-off rate. Figure 5.9 showcases the phished data that the Hotjar user behavior tracking tool recorded.

5.10 Phished User Movements on Desktop

This image records a snapshot showing detailed mouse movement across the landing page. It shows whether the user behavior is evaluating the page or reacting to the email received and

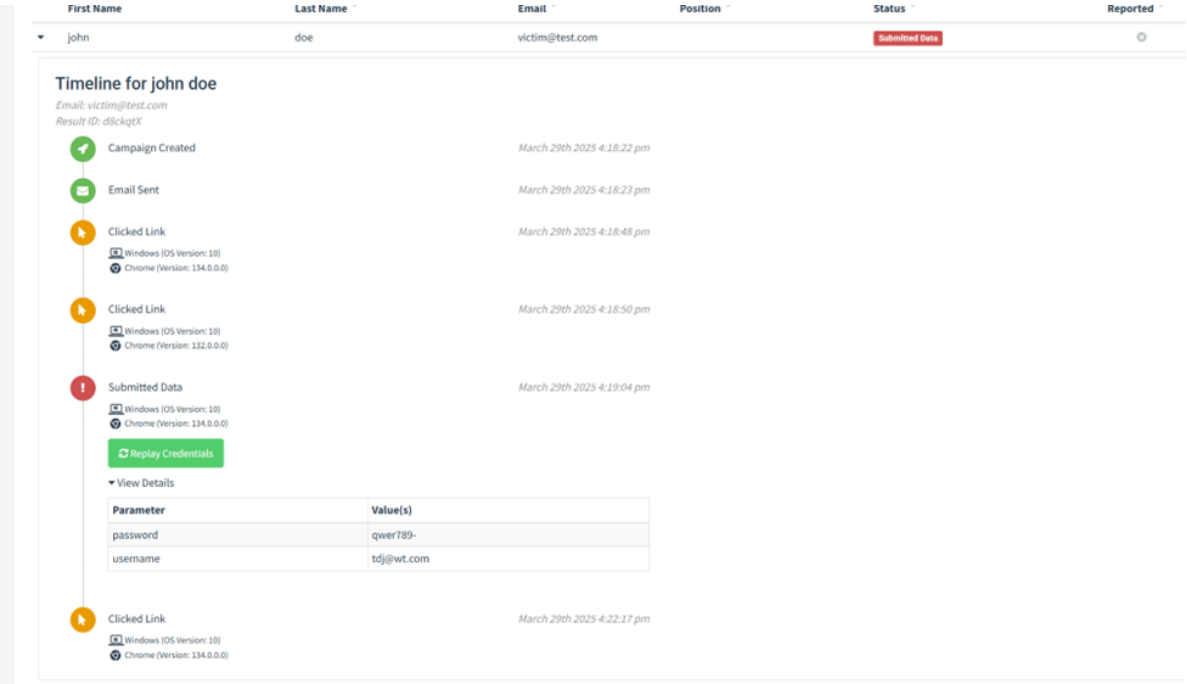

Figure 5.6 User Phished Data-Demo Campaign

filling in the details. Figure 5.10 showcases the user behavior movements captured by the Hotjar tool during the phishing simulation.

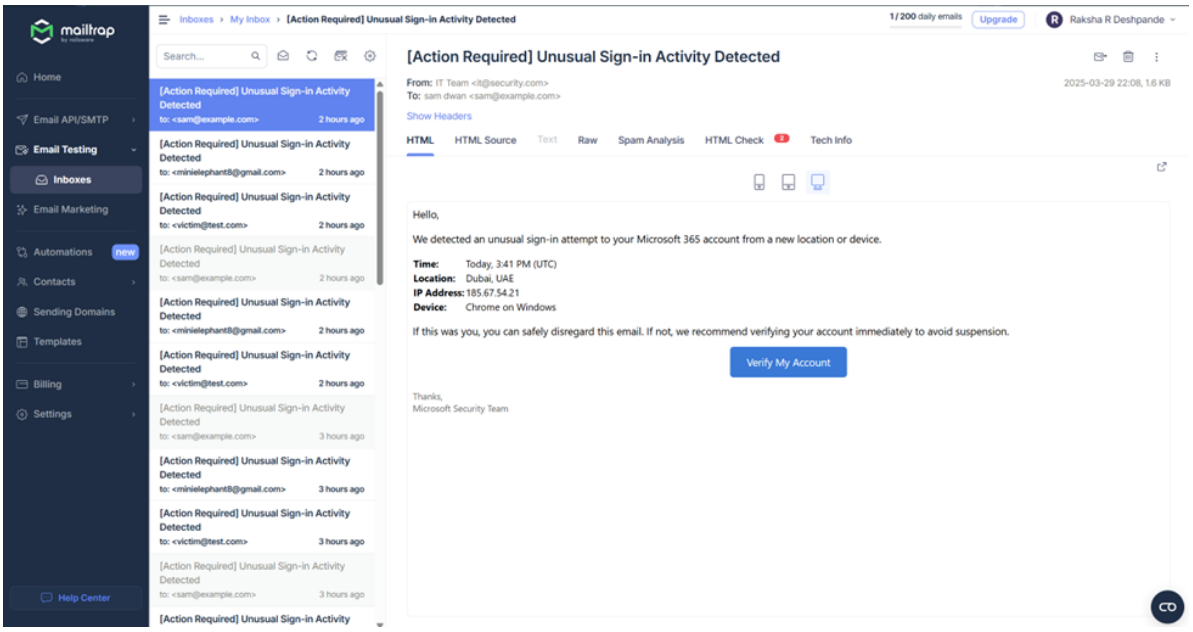

Figure 5.7 MAILTRAP SMTP: User Test Emails

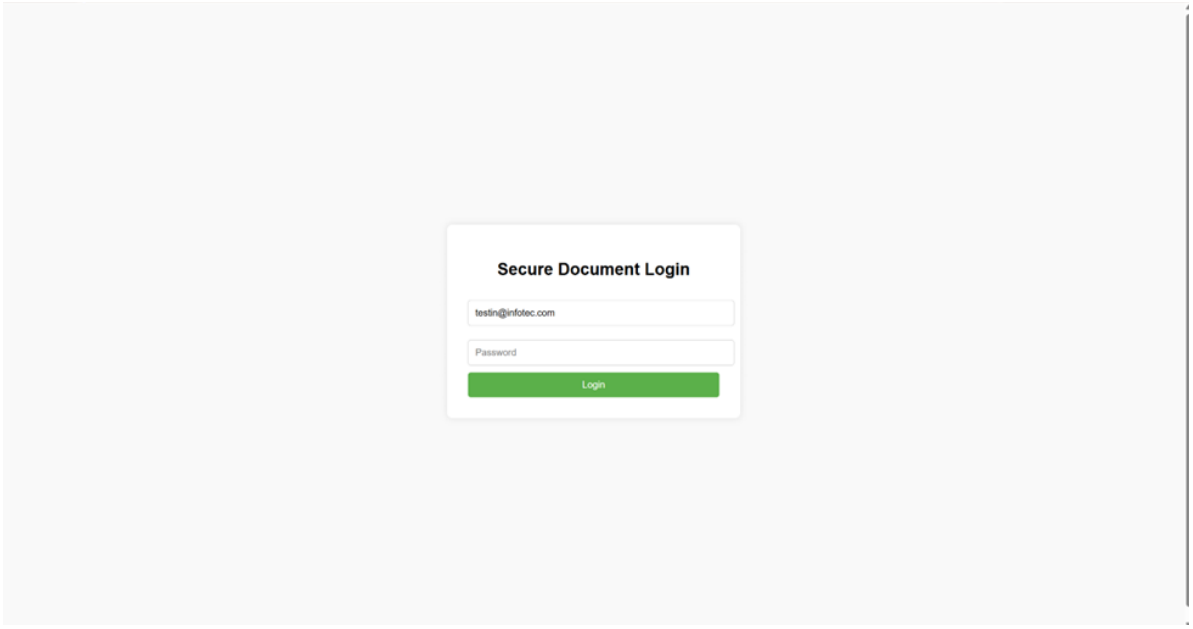

Figure 5.8 Google-Fake Login Page

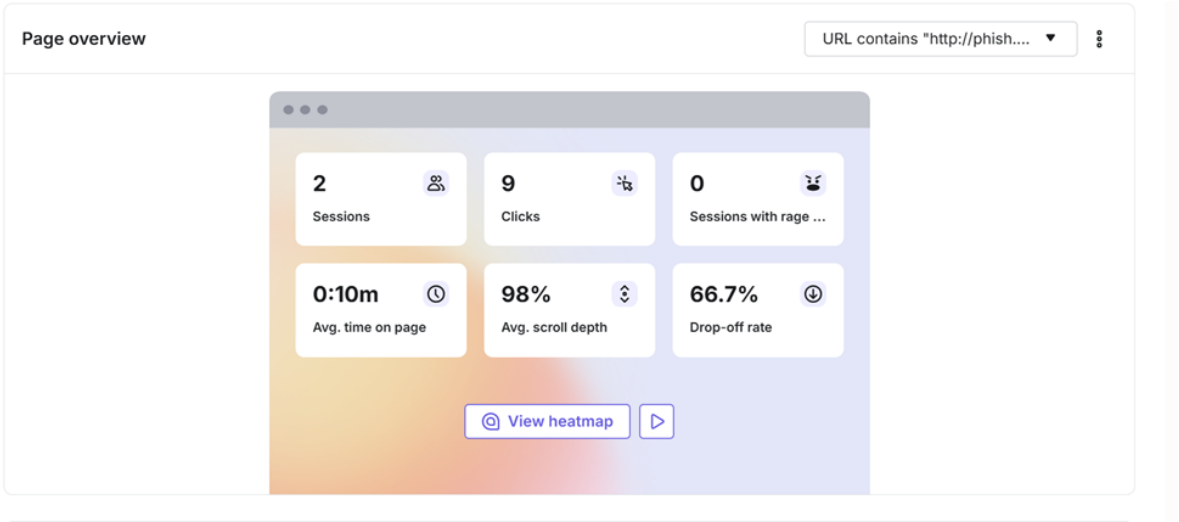

Figure 5.9 Hotjar-Phished User Behavior Overview

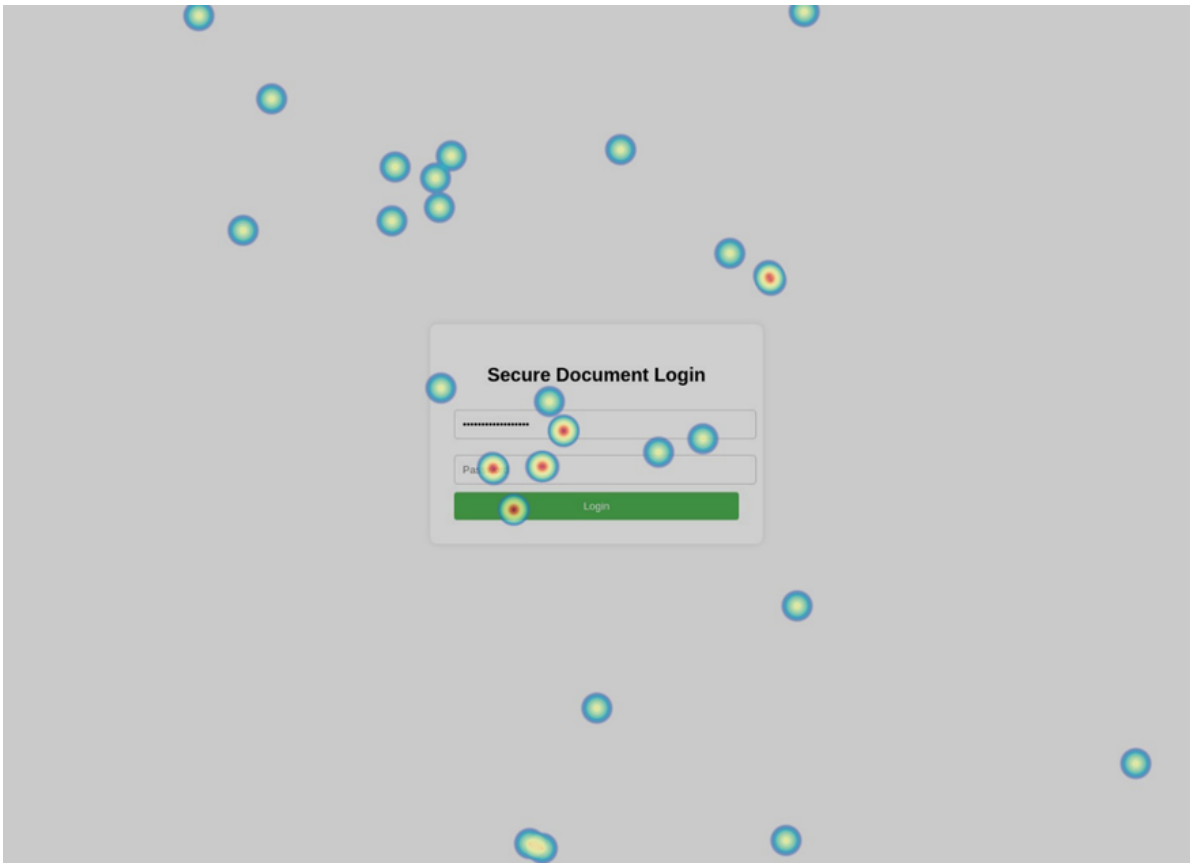

Figure 5.10 Phished User Movements on Desktop

CHAPTER 6. AWARENESS AND TRAINING IMPACT

I've developed and initiated various awareness strategies during this advanced phishing simulation project, which is summarized in this chapter. Traditional static training was not the sole emphasis of my work; I wanted to break the mold and focus on creating a more dynamic behavior model that reflects the manner in which users respond to phishing content. I designed learning that tracked individual user behavior, utilized visual feedback, and customized opportunities. With all of these educational experiences, I could observe and prompt positive shifts in user awareness and response.

6.1 Awareness Strategies Implemented

In order to improve user awareness and resilience skills against phishing, I designed a defined approach to solicit informed user engagement, tracking behaviors, and feedback specific to each user, which included the following steps:

- Simulated Realistic Phishing Scenarios: I designed phishing emails in a recognizable format that would mimic a phishing email. I included using a high level of urgency, indicating a potential security threat, to update user passwords. I was also mindful of the format and appearance of the emails. I sent the emails using Gophish, however, I routed them through Mailtrap to allow for testing without engaging the real site or any real stakeholders.

- Utilizing Hotjar for Tracking Behaviors in the Phishing Attach Scenarios: I embedded Hotjar scripts onto each phishing landing page to track user interactions. I was able to track how users moved their cursor around the page and how they clicked, scrolled, and interacted with thorough field attachments. Hotjar allowed me to analyze user hesitation, exploration, and instant results of the potential to fall to a phishing testing site. Risk-Based Behavior Identification - High Risk, Moderate Risk, Low-Risk Users: After reviewing the Hotjar

session recordings and Gophish tracking data, I was able to assign each user to one of the three flagged behavior profiles the user engaged with - High Risk, Moderate Risk, or Low Risk. This identification was useful in determining who needed additional training enhancements to bolster knowledge and who engaged in cautious behavior.

- Individualized User Feedback Development: I was able to put together visual representations of reports for each user using heat maps and session summaries. The purpose of each report was to outline risks and why certain actions put users at risk, as well as the next steps on how not to fall for phishing in future attempts.

- Providing Follow-Up Awareness Recommendations: Providing the required and right training to the users in universities and organizations helps to be aware of and reduce phishing attempts. Each department should undergo serious training regarding email phishing. Awareness regarding phishing should be taken serious and implemented widely across universities and organizations.

6.2 Why this Awareness Technique is More Effective

In my experience implementing this system, I observed it to be more effective than traditional training models. Here's why:

- Learning Through Simulation: Users were confronted with realistic phishing threats that they needed to respond to without notice. This provided me with an accurate gauge of user's awareness; plus it offered the users an effective learning experience founded in direct experience.

- Contextualized Feedback: By providing users with their actual click trail, scroll action, and heatmap, I provided visualizations that linked to them. I did not simply provide recommendations, I offered them feedback based on their personal actual behaviors.

- Engagement through Visualization: Users had a highly positive response to the heatmaps and session recordings. Many reported awareness of how quickly or impulsively they reacted

based on their own click path. Visualization also enhanced their understanding of their vulnerabilities.

CHAPTER 7. FUTURE WORK AND CONCLUSION

Although the simulation tool successfully merged realistic imitation of a phishing attack with real-time behavior tracking and contextual training, we are aware that this work has many possibilities to be advanced and continued. Future implementations should focus on scaling the simulation across larger and more diverse user groups in order to capture a wider spectrum of behavior patterns in order to further validate the risk profiling model. Longitudinal studies are also critical to monitor how user awareness changes over time and whether gains in retention improve in individuals who have participated in a second or third simulation. Likewise, further analytics that could provide enhanced individual modeling using machine learning, such as predictive risk scoring and automated responses to training, could expand the personalization and learning. Finally, launching the platform beyond email to simulate phishing by SMS, messaging apps, or voice phishing (vishing) would present a more complete and real-life training ecosystem reflective of the current phishing landscape. This project reaffirmed the importance of behavioral insights in phishing detection and awareness training. By modifying our metrics from generic reports to heatmaps, scroll depth, and individual user actions, the tool demonstrated user engagement with various phishing attempts in a more meaningful way. The ability to provide visual, personalized feedback strengthened user engagement and developed a deeper understanding of the risk of phishing engagements. This project encapsulated a unique combination of Gophish, Mailtrap, and Hotjar that produced an ethical model that was practical for the organization and informative for the researcher to use as a simulation. This project demonstrates that utilizing user behavioral analytics in conjunction with training about risks related to phishing allows for a powerful approach to improving cybersecurity and phishing awareness at the individual, university, and organizational levels.

BIBLIOGRAPHY

[1] Luigi Gallo, Danilo Gentile, Saverio Ruggiero, Alessio Botta, and Giorgio Ventre. The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, 139:103671, 2024.

[2] Ziad M. Hakim, Natalie C. Ebner, Daniela S. Oliveira, Sarah J. Getz, Bonnie E. Levin, Tian Lin, Kaitlin Lloyd, Vicky T. Lai, Matthew D. Grilli, and Robert C. Wilson. The phishing email suspicion test (pest) a lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behavior Research Methods*, 53(3):1342–1352, Oct 2020.

[3] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. A phishing mitigation solution using human behaviour and emotions that influence the success of phishing attacks. In *Adjunct proceedings of the 29th ACM conference on user modeling, adaptation and personalization*, pages 345–350, 2021.

[4] Nathan Beu, Asangi Jayatilaka, Manssoreh Zahedi, Muhammad Ali Babar, Laura Hartley, Winston Lewinsmith, and Irina Baetu. Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. *Computers & Security*, 131:103313, 2023.

[5] Julie S Downs, Mandy Holbrook, and Lorrie Faith Cranor. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 37–44, 2007.

[6] Yan Ge, Li Lu, Xinyue Cui, Zhe Chen, and Weina Qu. How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics*, 97:103526, 2021.

[7] Ahmed Abbasi, David Dobolyi, Anthony Vance, and Fatemeh Mariam Zahedi. The phishing funnel model: a design artifact to predict user susceptibility to phishing websites. *Information Systems Research*, 32(2):410–436, 2021.

[8] Yi Yong Lee, Chin Lay Gan, and Tze Wei Liew. Thwarting instant messaging phishing attacks: the role of self-efficacy and the mediating effect of attitude towards online sharing of personal information. *International Journal of Environmental Research and Public Health*, 20(4):3514, 2023.

[9] Kibreab Adane and Berhanu Beyene. Email and website-based phishing attack: examining online users security behavior in cyberspace environment. *International Journal of Information Science and Management (IJISM)*, 21(1):245–262, 2023.

[10] Sivaraju Kuraku, Dinesh Kalla, Nathan Smith, and Fnu Samaah. Exploring how user behavior shapes cybersecurity awareness in the face of phishing attacks. *International Journal of Computer Trends and Technology*, 2023.

[11] Rundong Yang, Kangfeng Zheng, Bin Wu, Di Li, Zhe Wang, and Xiujuan Wang. Predicting user susceptibility to phishing based on multidimensional features. *Computational Intelligence and Neuroscience*, 2022(1):7058972, 2022.

[12] Dennik Baltuttis and Timm Teubner. Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment. *Computers & Security*, 144:103940, 2024.

[13] Abdullah Alshehri, Nayeem Khan, Ali Alowayr, and Mohammed Yahya Alghamdi. Cyberattack detection framework using machine learning and user behavior analytics. *Computer Systems Science & Engineering*, 44(2), 2023.

[14] Asmaa Reda Omar, Shereen Taie, and Masoud E Shaheen. From phishing behavior analysis and feature selection to enhance prediction rate in phishing detection. *International Journal of Advanced Computer Science and Applications*, 14(5), 2023.

[15] Medhasree Ghosh, Dyuti Ghosh, Raju Halder, and Joydeep Chandra. Investigating the impact of structural and temporal behaviors in ethereum phishing users detection. *Blockchain: Research and Applications*, 4(4):100153, 2023.

[16] Anargyros Chrysanthou, Yorgos Pantis, and Constantinos Patsakis. The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign. *Computers & Security*, 140:103780, 2024.

[17] Rui Chen, Joana Gaia, and H Raghav Rao. An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, 133:113287, 2020.

[18] Muhammad Nadeem, Syeda Wajiha Zahra, Muhammad Nouman Abbasi, Ali Arshad, Saman Riaz, and Waqas Ahmed. Phishing attack, its detections and prevention techniques. *Int. J. Wirel. Secur. Netw*, 1:13–25, 2023.

[19] Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius, and Cate Jerram. The design of phishing studies: Challenges for researchers. *Computers & Security*, 52:194–206, 2015.

[20] Diego Esteban Díaz Vivas, William Yecid Gutierrez Pena, and Sandra Patricia Cristancho. A controlled phishing attack in a university community: A case study. *Journal of Internet Services and Information Security (JISIS)*, 14(2), 2024.

[21] Amy E Antonucci, Yair Levy, Laurie P Dringus, and Martha Snyder. Experimental study to assess the impact of timers on user susceptibility to phishing attacks. *Journal of Cybersecurity Education, Research and Practice*, 2021(2):6, 2022.

[22] Matthew Shonman, Xiaoyu Shi, Mingqing Kang, Zuo Wang, Xiangyang Li, and Anton Dahbura. Using a computational cognitive model to understand phishing classification decisions of email users. *Interacting with Computers*, 36(2):113–125, 2024.

[23] Orvila Sarker, Asangi Jayatilaka, Sherif Haggag, Chelsea Liu, and M Ali Babar. A multi-vocal literature review on challenges and critical success factors of phishing education, training and awareness. *Journal of Systems and Software*, 208:111899, 2024.

[24] Giuseppe Desolda, Lauren S Ferro, Andrea Marrella, Tiziana Catarci, and Maria Francesca Costabile. Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, 54(8):1–35, 2021.

[25] Frank L Greitzer, Wanru Li, Kathryn B Laskey, James Lee, and Justin Purl. Experimental investigation of technical and human factors related to phishing susceptibility. *ACM Transactions on Social Computing*, 4(2):1–48, 2021.

[26] Het Patel, Umair Rehman, and Farkhund Iqbal. Evaluating the efficacy of large language models in identifying phishing attempts. In *2024 16th International Conference on Human System Interaction (HSI)*. IEEE, 2024.

[27] R Septiana and RK Julian. Design of phishing simulation dashboard using analytic data concepts. *Journal of Physics: Conference Series*, 1577(1), 2020.

[28] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. The effects of group discussion and role-playing training on self-efficacy, support-seeking, and reporting phishing emails: Evidence from a mixed-design experiment. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024.

[29] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. Don't click: towards an effective anti-phishing training. a comparative literature review. *Human-centric Computing and Information Sciences*, 10(1), 2020.

[30] Sarah Y Zheng and Ingolf Becker. Checking, nudging or scoring? evaluating e-mail user security tools. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 57–76, 2023.