Reducing Phish-Prone By Simulated Attacks And Trainings

by

Muhammad Ahsan Shakeel

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

May 2023

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Muhammad Ahsan Shakeel**, Registration No. **00000319363**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: Asst Prof Dr. Mian Muhammad Wassim Iqbal

Date: _____

HoD
Information Security
Military College of Sig

Signature (HOD): _____

Date: _____

Signature (Dean/Principal) _____

Date: 5/7/23

Brig
Dean, MCS (NUST)
(Asif Masood, Phd)

Declaration

I hereby declare that no portion of the work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

__**Muhammad Ahsan Shakeel**
MS Student

Dedication

“In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my parents, and teachers who supported me every step of the way.

Acknowledgments

All praises to Allah for the strengths and His blessing in completing this thesis.

I would like to convey my gratitude to my supervisor, Assoc Prof Dr. Mian Muhammad Waseem Iqbal, for his supervision and constant support. His invaluable help of constructive comments and suggestions throughout the experimental and thesis works are major contributions to the success of this research. Also, I would like to thank my committee members, Asst. Prof Dr Yawar Abbas, and Asst. Prof Dr. Waleed Bin Shahid for their support and knowledge regarding this topic.

Last, but not the least, I am highly thankful to my parents. They have always stood by my dreams and aspirations and have been a great source of inspiration for me. I would like to thank them for all their care, love and support through my times of stress and excitement.

Abstract

Phishing attacks continue to be a pervasive and serious cybersecurity threat, exploiting human vulnerability and causing significant financial and reputational damage. This thesis presents the development and evaluation of a comprehensive phishing simulation and awareness tool that integrates Cialdini's principles of persuasion and elements of a cyber drill. The primary objective is to reduce individuals' susceptibility to phishing attacks by providing realistic simulations, targeted training, and reinforcing the principles of persuasion.

The thesis begins with a thorough exploration of Cialdini's principles of persuasion, including reciprocity, authority, commitment/consistency, social proof, liking, and scarcity. These principles serve as a theoretical foundation for designing persuasive phishing simulations payloads that exploit human cognitive biases and decision-making processes, thereby increasing users' awareness of social engineering techniques.

Drawing upon this theoretical framework, a phishing simulation and awareness tool is developed, incorporating a variety of persuasive strategies and utilizing realistic phishing techniques. The tool enables users to experience simulated phishing attacks in a controlled environment, providing immediate feedback and educational resources to enhance their understanding and response to such threats. By analyzing user interactions and behavior patterns, the tool generates comprehensive reports that identify specific areas for improvement in users' phishing awareness and response.

To further strengthen users' preparedness, the tool incorporates elements of a cyber drill, creating an engaging and gamified learning experience. Participants are exposed to targeted trainings based on their performance in simulated phishing campaigns. The tool employs interactive modules, immediate feedback, and adaptive learning techniques to reinforce users' knowledge and decision-making skills, fostering a proactive and resilient approach to phishing threats.

The effectiveness of the developed tool is evaluated through a series of controlled experiments involving participants with varying levels of cybersecurity awareness. The evaluation focuses on measuring the reduction in participants' susceptibility to phishing attacks after engaging with the simulation and awareness tool. Additionally, user feedback and qualitative analysis are collected to assess the tool's usability and effectiveness in improving users' resilience against phishing threats.

The results of the study demonstrate the efficacy of the phishing simulation and awareness tool in reducing individuals' phish-prone behavior. The findings highlight the positive impact of integrating Cialdini's principles of persuasion and cyber drill techniques, revealing a significant improvement in participants' phishing awareness, decision-making skills, and resistance to social engineering attempts. This research contributes to the field of cybersecurity by offering a practical and effective approach to mitigating the risks associated with phishing attacks, ultimately enhancing the overall cybersecurity posture of individuals and organizations.

Keywords: Phishing, simulated attacks, Security Awareness Training, Phish Prone Behavior

Table of Contents

Page

Table of Contents

List of Figures

LIST OF TABLES

ACRONYMS

Phish-Prone Percentage	PPP
Analysis of Variance	ANOVA
Out-Of-The-Box	OOTB
Percentage Change Rate	PCR
Finite State Machine	FSM

Chapter 1

Introduction

1.1 Overview

With the exponential growth of technology and the internet, the threat of cybercrime has risen significantly, causing enormous financial losses, as well as major disruptions in the operations of businesses and organizations worldwide. Phishing attacks are one of the most common types of cybercrime, and they are becoming increasingly sophisticated, making them difficult for organizations to defend against. Phishing is causing multi-billion-dollar losses to enterprises and end-users [1]. Phishing attacks typically involve the use of social engineering techniques to manipulate victims into divulging confidential information, such as login credentials, financial information, and personal details. The phishing attack is an attack on people [2]. Despite the significant impact of phishing attacks, many organizations struggle to combat them effectively. Training employees to identify and avoid phishing attacks has been a common approach, but traditional training programs often fail to provide realistic simulations of actual phishing attacks. This makes it difficult for employees to recognize and respond appropriately to real phishing emails.

Recent research suggests that simulated attacks and training may be more effective in reducing phish-prone behavior. Exposing employees to realistic phishing scenarios, simulated attacks, and training can improve employees' awareness of phishing scams and their ability to recognize and avoid them. This approach has gained popularity in recent years, and many organizations are now using it to complement traditional training programs. Phishing awareness campaigns are becoming increasingly urgent [5]. The objective of this study is to evaluate the effectiveness of simulated attacks and training in reducing phish-prone behavior and to identify the factors that influence phish-prone behavior. The percentage of an organization's workforce that falls for phishing assaults is referred to as the "phish-prone percentage" (PPP) [9].

Verizon's 2018 data breach investigation report found that 93% of data breaches were the result of phishing or other forms of social engineering. Phishing attacks continue to be a significant threat to individuals and organizations alike. These attacks involve the use of deceptive emails, websites, or other digital communications to trick recipients into divulging sensitive information or performing actions that could compromise their

cybersecurity. Despite the increasing awareness of the dangers of phishing, many individuals and organizations still fall victim to these attacks, often due to a lack of awareness, training, or effective prevention measures. The below Figure 1 demonstrate how phishing attack works.

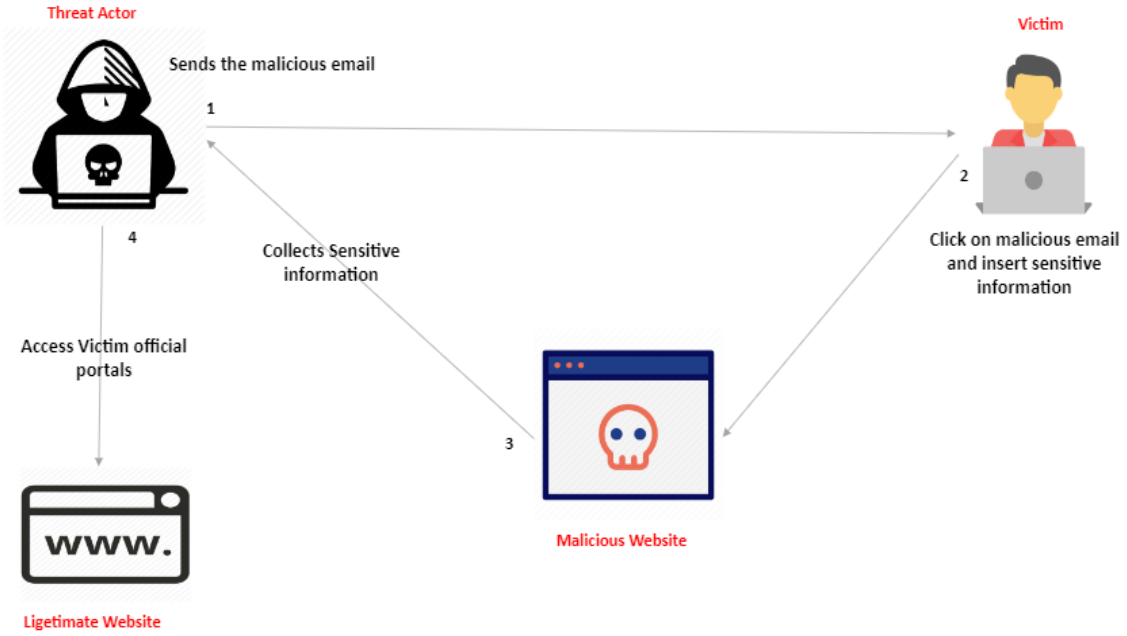

Figure 1.1: Phishing Attack Workflow

In response to this ongoing threat, researchers and cybersecurity professionals have developed a range of strategies for reducing the likelihood of phishing attacks succeeding. One promising approach involves the use of simulated phishing attacks and training programs to educate individuals and organizations about the dangers of phishing and help them develop more effective strategies for recognizing and avoiding these scams.

The goal of this thesis is to investigate the effectiveness of simulated phishing attacks and training programs in reducing phish-prone behavior. To achieve this goal, the study will utilize a combination of qualitative and quantitative research methods to examine the impact of these interventions on participants' awareness, knowledge, and behavior related to phishing attacks.

By exploring the efficacy of these strategies, this thesis aims to contribute to a better understanding of how to prevent and mitigate the risks of phishing attacks. Ultimately,

the findings of this study may inform the better and more effective development of a tool that provides guidelines about how effective phishing risk assessment can be done and how organizations can reduce their end-user susceptibility to phishing attacks through security awareness programs.

One approach to reducing the risks of phishing attacks is through simulated attacks and training programs. Simulated attacks involve sending fake phishing emails or messages to individuals or groups, to test their susceptibility to these scams and educate them on how to avoid them in the future. The phishing awareness strategy aims to educate users so they can recognize phishing e-mails and take appropriate action [4]. While some studies have shown that simulated attacks and training programs can be effective in reducing phish-prone behavior, others have found that they may have limited or short-term impact, or may even lead to a false sense of security among participants. As such, further research is needed to understand better the potential benefits and limitations of simulated attacks and training programs to reduce phishing attacks' risks. This thesis seeks to contribute to this vital area of research by examining the impact of these interventions on participants' awareness, knowledge, and behavior related to phishing attacks.

1.2 Research Aims and Questions

Research Aims:

We focused on the human factors of awareness through the simulation's attacks and interactive video training and evaluated their understanding using interactive challenges. We also focused on calculating the phish-prone percentage by each user, organization, and industry benchmark.

Research Questions:

The followings are the research questions:

- How effective are simulated attacks and training in reducing phish-prone behavior among employees?
- What are the current awareness, knowledge, and behavior levels related to phishing attacks among the target population?
- How effective are simulated phishing attacks in increasing awareness and reducing susceptibility to phishing attacks?
- How effective are training programs in increasing knowledge and promoting positive behaviors related to phishing attacks?

- What are the key factors that influence the effectiveness of simulated attacks and training programs, including participant characteristics, message content, and delivery method?
- Are there any unintended consequences of simulated attacks and training programs, such as increased anxiety or decreased productivity?
- To what extent do simulating attacks and training increase employees' ability to recognize and avoid phishing emails?
- What is the optimal frequency of simulated attacks and training for maintaining a high level of phish-prone behavior reduction among employees?
- What are the best practices for implementing and conducting simulated attacks and training in an organizational setting?

1.3 Objectives

The main objectives of the thesis are:

- Proposing new anti-phishing techniques based on human factors.
- Develop an Anti-Preparing simulation tool that contains training videos for awareness and evaluation.

1.4 Thesis Contribution

The main contributions of this work are as follows.

- The study will provide insights into the current levels of awareness, knowledge, and behavior related to phishing attacks among the target population, which can help identify areas for improvement and inform the development of more effective phishing prevention strategies.
- The study will evaluate the effectiveness of simulated attacks and training programs in reducing phish-prone behavior, providing valuable evidence-based guidance to individuals and organizations looking to implement these interventions.
- The study will identify key factors that influence the effectiveness of simulated attacks and training programs, including participant characteristics, message content, and delivery method. This information can be used to optimize the design and delivery of future interventions and improve their overall effectiveness.

- The study will assess the potential unintended consequences of simulated attacks and training programs, such as increased anxiety or decreased productivity, and provide recommendations for mitigating these effects.
- The study will contribute to the broader literature on phishing prevention by providing empirical evidence on the effectiveness of simulated attacks and training programs and identifying gaps in our understanding of this important area of research.

1.5 Applications

The findings of this thesis have a range of potential applications for individuals, organizations, and policymakers looking to prevent and mitigate the risks of phishing attacks. Some of the critical applications include:

Training and education programs: The study provides evidence-based guidance on the design and delivery of effective training and education programs for preventing phishing attacks. Sun, Yu, Lin, and Tseng stated that increasing users' security knowledge can reduce the possibility of phishing e-mails deceiving them [6]. These programs can help individuals and organizations develop the knowledge, skills, and resources needed to recognize and avoid phishing scams, ultimately reducing the risks of cybercrime and other forms of cyberattacks.

Security policies and practices: The study can inform the development of more effective security policies and practices related to email security, password management, and other cybersecurity measures. By understanding the factors that influence the effectiveness of simulated attacks and training programs, policymakers can develop policies that promote best practices and improve the overall cybersecurity posture of organizations.

Technology and tool development: The study can inform the development of new technologies and tools for detecting and preventing phishing attacks. By SpoofStick, Netcraft, and SpoofGuard, these tools are not the only means to develop to detect and prevent phishing attacks [3]. With technology enhancement organizations also need human security awareness to protect the last layer of defense by educating them.

Organization Type	Potential Benefits
Small businesses	Improved employee awareness and behavior related to phishing attacks, reduced risk of financial loss and data breaches
Large corporations	Reduced risk of corporate data breaches and other forms of cybercrime, improved employee awareness and behavior related to phishing attacks.
Educational institutions	Improved student and faculty awareness and behavior related to phishing attacks, reduced risk of data breaches and cyberattacks.
Healthcare organizations	Improved staff awareness and behavior related to phishing attacks, reduced risk of data breaches and other forms of cybercrime.
Government agencies	Improved official awareness and behavior related to phishing attacks, reduced risk of state data breaches and cyberattacks.

Table 1.1. Implementation of Work

Overall, the applications of this thesis are broad and far-reaching, with potential benefits for a wide range of organizations and individuals. By advancing our understanding of how to prevent and mitigate the risks of phishing attacks, this study has the potential to improve cybersecurity for all.

1.6 Research Methodology

In this research, we use a systematic literature review approach. In the systematic literature review, several article sources are used, including Science Direct, IEEE Xplore, Google Scholar database, and Springer. Studies are selected after reading titles, abstracts, introductions, and conclusions to decide whether the articles are peer-

reviewed, and relevant to the subject. A case study is used to validate and identify which workflow and awareness programs are being used for phishing awareness. The comparison of phishing awareness program workflow and methodologies is conducted to identify the commonalities and gaps and propose a newly enhanced tool is built to fulfill all the gaps of the existing program.

1.7 Problem Statement

Phishing attacks are becoming increasingly sophisticated and are a significant threat to organizations and their employees. Despite the growing awareness of these attacks, many employees still fall prey to phishing scams, which can lead to data breaches, financial losses, and reputational damage. This highlights the need for effective strategies to reduce phish-prone behavior in organizations. Current approaches to reducing phish-prone behavior often involve providing employees with basic training on recognizing and avoiding phishing attacks. However, these approaches have limited effectiveness, as need to-do does not address the underlying factors that contribute to phish-prone behavior. In addition, traditional training programs may need to be more engaging and tailored with time, which can result in low adoption rates and limited effectiveness. This research presents the development and evaluation of a comprehensive phishing simulation and awareness tool that integrates Cialdini's principles of persuasion and elements of a cyber drill. The primary objective is to reduce individuals' susceptibility to phishing attacks by providing realistic simulations, targeted trainings, and reinforcing the principles of persuasion.

1.8 Thesis Organization

The thesis is structured as follows:

- **Chapter 1 - Introduction**: In the introduction, we will provide background and context for your study on reducing phish-prone behavior through simulated attacks and training. We will state our research problem and objectives, research questions and hypotheses, and the significance and contributions of the study. We will also describe the scope and limitations of the study.
- **Chapter 2 - Literature Review and Existing Methodologies**: In the literature review, we will provide an overview of phishing attacks and their impact on organizations. We will review previous studies on the effectiveness of simulated attacks and training in reducing phish-prone behavior, and describe the

theoretical frameworks and models related to phish-prone behavior and cybersecurity awareness. We will also review studies on the factors that influence phish-prone behavior, including personality and cognitive factors.

- **Chapter 3 – Proposed Methodology**: In the methodology section, we will describe our research design and approach, sampling strategy and participants, data collection methods and instruments, and data analysis techniques and procedures. We will also discuss ethical considerations in our research.
- **Chapter 4 – Experimental Setup and Scenario:** In this section, we will describe the proposed tool UI and explain the scenario to company x. How to use the proposed tool to calculate the current phishing risk state as well as the awareness progress.
- **Chapter 5 – Results and Scenario:** In the results section, we will present descriptive statistics and characteristics of the sample and analyze the effectiveness of simulated attacks and training in reducing phish-prone behavior. We will also analyze the factors that influence phish-prone behavior and compare results between groups and subgroups.
- **Chapter 6 – Discussion, Conclusion, and Future Work:** In this section, we will interpret our results and findings, and discuss the implications for theory and practice. We will describe the limitations of your study and suggest future research directions. Finally, will summarize our study and its contributions, and discuss the implications for organizations and policymakers. You will provide a conclusion and final thoughts on the topic of reducing phish-prone behavior through simulated attacks and training. Also, we will provide complete insights about our future work in this thesis.

Chapter 2

Literature Review and Existing Methodology

In this section, we will discuss the concepts of phishing, also analyzed the related work in the literature work, and highlight the research gaps. A proper review of existing work and adopted methodologies will also discuss how current work is enhancing human awareness against phishing attacks and providing guidelines to reduce the Phish-Prone percentage (PPP) [9] of the organization. This section covers the literature review and also the existing methodologies to address the gaps and improvements.

2.1 Literature Review

Phishing attacks utilize social engineering techniques to craft messages to deceive victims into taking actions such as opening attachments, clicking on embedded hyperlinks, or providing sensitive information [8]. These attacks are typically conducted via email, but can also occur through social media, messaging apps, or other channels. Phishing attacks have become increasingly sophisticated in recent years, with attackers using advanced techniques such as spear-phishing and whaling to target specific individuals or organizations. Phishing attacks can have serious consequences for individuals and organizations. In addition to financial losses and data breaches, successful phishing attacks can result in reputational damage, legal liabilities, and regulatory fines. Despite the growing awareness of these risks, many individuals and organizations still need to catch up to phishing attacks.

Even though phishing attempts are expensive for businesses and individuals alike, existing academic research has provided little direction on how to organize and conduct a combined phishing awareness and training campaign. Through an in-depth case study of a massive phishing awareness campaign, author showed that phishing awareness is a learning process that can be used to promote positive behavior and deter undesirable actions. This study [12] heavily incorporate insights from the operant conditioning theory. Based on the results of the case study, author presented a wide variety of suggestions aimed at various cybersecurity industry players. This research adds to what has already been done to improve people's ability to spot and avoid phishing attempts, and it also suggests avenues for further study and changes to current procedures. This

document is useful for businesses who are developing, launching, or revising a phishing awareness and education initiative.

In this study [20], phishing simulations used as part of ongoing cybersecurity awareness training have resulted in a general trend towards lower click rates. Based on an examination of a sample of 215 mid-sized organizations in May 2018 with similar demographics, author found that if you phish your employees once a year, this organization will have a 27% susceptibility rate. Instead, it utilized PhishProof phishing attempts once a month, your exposure drops to a mere 4%.

The number of phishing emails sent to workers has increased, especially as more individuals start doing remote work. For the Greathorn, the year 2020 Scenery of online phishing attacks. In this study [18], author looked at why and how phishing email attacks have grown so pervasive and harmful. Author looked into the current features of phishing assaults, with a special emphasis on the increasing issues that have arisen as a result of the COVID-19 outbreak. The report describes a study wherein five distinct email formats (both phishing and non-phishing) were shown to participants. Findings from the study show that most people are unable to recognize modern phishing emails. Participants in the study were asked to pay special attention to any emails they received that were out of the ordinary, such as those with grammatical or spelling mistakes or those that asked for personal information. The author also learned that people have little trust in, are afraid of, and are overall dissatisfied with the status of phishing email protection. These feelings alerted us to the growing gravity of the phishing attack scenario and the continued precariousness of modern society.

The study set out to examine whether or not a phishing training program at a single, unnamed healthcare organization in the United States lowered the number of times healthcare employees at the organization fell for a phishing scam. The author made a clear distinction between those who break the law and those who don't. Offenders in this study were defined as those who opened at least 5 simulated phishing emails, whereas non-offenders were those who did not meet this threshold. In this study [14] author examined click rates of offenders and non-offenders before and after a mandatory training program for offenders was implemented. There were 5,416 workers who received all 20 communications throughout the intervention period, and 772 of them were considered repeat offenders since they saw more than five emails. Out of the 3,564 people in this sample, just 975 (17.1%) clicked on zero phishing emails across all 20

campaigns, whereas 3,565 (65.3%) clicked at least two. Click through rates fell uniformly across all 20 campaigns. In spite of the mandatory training program being put in place after campaign 15, the click rates barely budged, and repeat offenders were still more likely to fall for a phishing simulation. Phishing is a common attack vector against hospital employees and a major cybersecurity issue for healthcare organizations. Research in this field shows that employees' click rates go down with more exposure to simulation, but that a mandatory training program designed for high-risk individuals had little effect on click rates. Clicks on phishing emails from employees have decreased over time, but mandatory training for high-risk employees has not reduced their chance of clicking.

The percentage of successful phishing attacks is at an all-time high, and the available technical solutions aren't enough to combat this trend. Consumers must be taught to recognize phishing attempts in their inbox’s, therefore anti-phishing education is vital. Author [17] used a 22 factorial arrangement to compare the effectiveness of instructor-led classroom training to that of a multiple approach video-, game-, and text-based training package, as well as to that of no training at all. The results show that measures to lessen susceptibility to phishing that include classroom training are only partially successful. In addition, if given the option to select from a variety of training techniques, participants virtually universally prefer classroom education.

Several methods have been explored in previous research aimed at increasing employee awareness and decreasing their susceptibility to phishing using simulated attacks and training. Research into how to best raise awareness and decrease susceptibility to phishing attempts has focused on both training program development and delivery, as well as on the use of simulated attacks. Although these studies show that these methods are successful in decreasing phish-prone behavior, more research is needed to determine which methods are most useful in various business settings. Also, there is a requirement for more all-encompassing techniques that account for the different aspects that lead to phish-prone behavior, such as personality characteristics, organizational culture, and the ever-changing nature of phishing attempts. The current [13] study's overarching goal is to fill in these blanks by developing an all-encompassing anti-phishing methodology that integrates simulated attacks, individualized training

programs, employee buy-in, monitoring and feedback, and executive support to foster a culture of security and lessen the likelihood of falling victim to phishing attacks.

It's no secret that phishing assaults, which use social engineering to get access to private information, are common in the healthcare industry. A simulated attack is an effective way to evaluate an organization's preparedness for a phishing attack. It may be more difficult to recognize a phishing email if you are fatigued or if the fake message is particularly intricate. A large Italian hospital with over 6,000 employees ran a phishing simulation as part of its annual training and risk assessment. Three campaigns, spaced around every four months, were run to compare the efficacy of generic versus personalized phishing emails among staff members. According to the findings, phishing emails are more successful when they are personalized. Yet, whereas only 38% of workers didn't open the personalized phish, 64% of those who received the generic phish didn't. The percentage of workers who clicked on the personalized ad also differed considerably. Yet, internal barriers prevented the campaigns from going off without a hitch. While phishing simulation tools might be helpful, they are not without potential drawbacks. Author needed the appropriate knowledge, abilities, and experience to get things done quickly and effectively. Throughout this Hospital simulation, some issues were raised. Ethical phishing campaigns require organization-wide coordination, precise timing, and a lack of staff understanding. [15] This requires careful coordination, which is not always easy. Misleading messages, such as those that overstate threats or give false assurances, can elicit unfavorable responses from workers and unions. Adapting the message to current events in the area increases the likelihood that it will reach its intended audience and has an effect. The knowledge learned can be used to healthcare settings throughout the world.

In this study, the author detailed the findings of a large-scale, multi-month phishing experiment that author conducted with an affiliated company. Over the course of the study's 15-month period, over 14,000 participants (all employees of the organization) were sent various simulated phishing emails while going about their regular workday. To further facilitate the reporting of spam, the author included a report button to the company's email client. The author kept tabs on how often people fell for phishing emails, what they did once they did, whether it was submit sensitive information or forward the message, and how often they reported it. Based on these findings, the author may offer three distinct contributions. To begin, the ecological reliability of the

background information has been improved thanks to this study. One result is that email warnings are effective. Second, the findings challenge long-held beliefs and popular understanding in the field. Unintentionally, the author found that the widespread practice of using simulated phishing exercises for training purposes makes workers more susceptible to phishing. Third, the author offered forth some new findings. More specifically, the author demonstrated the feasibility of deploying an organization's personnel as a centralized phishing detection system. This study [16] showed that this method of crowdsourcing is effective at detecting new phishing attempts in a short amount of time, with minimal impact on day-to-day operations, and with a high level of employee engagement.

Phishing is an easy method that can be used to bypass firewalls and other complex technical protections. It is frequently employed in social engineering attacks like ransomware to take advantage of psychological (and other) aspects of human users. A phishing simulation was done via short message service (SMS) among healthcare professionals in Ghana, with reference to the current state of the art in healthcare phishing simulation research and taking into account the inherent ethical constraints. Field observations, numerical questionnaires, and in-depth interviews were all a part of the research. The results of several studies have demonstrated that field research is far more effective than laboratory randomized controlled trials or statistical surveys. While 61% of the healthcare personnel targeted fell for the simulated phishing assault, there were some who put patient care first and were therefore immune to the attack. Using structural equation modelling, author [30] found that increased workload was a significant predictor of self-efficacy risk ($r = 0.5$, $p = 0.05$), whereas a work emergency was a predictor of a perceived barrier ($r = 0.46$, $p = 0.00$). Also, the perceived barrier was found to be a predictor of self-reported security behavior in phishing assaults among healthcare personnel as measured by Pearson's correlation. Hence, many recommendations were made to improve the staff's deliberate care behavior, such as increasing security training and the number of security measures in emergency rooms by 50%. [21]

2.2 Existing Methodologies

In this section, we will discuss existing methodologies for reducing phish-prone behavior through simulated attacks, and training programs typically involve a combination of several strategies. These can include:

2.2.1 Conducted Simulated Phishing Attacks

Simulated phishing attacks help organizations identify employees prone to phishing scams. Specific individuals or departments requiring additional training or support can be pinpointed by analyzing responses to fake phishing emails. These attacks play a vital role in anti-phishing methodologies, aiding in recognizing and avoiding genuine phishing attempts.

Simulated attacks resemble real phishing emails, employing authentic email addresses, logos, and content. Employees may be prompted to click on links, provide personal information, or open attachments. The system records track interactions, exposing potential weaknesses.

Analyzing results allows the identification of employees or departments needing extra training or support. For instance, if a department exhibits a high click rate, focused training can be provided to improve recognition and avoidance of actual phishing attacks. To minimize the risks associated with phishing and safeguard businesses, organizations, and individuals from phishing attacks, it is crucial to comprehend the factors that influence susceptibility to phishing schemes. This understanding serves as a foundation for developing effective countermeasures [29]. Simulated attacks establish a vulnerability baseline, allowing tracking of improvements over time. Regular simulated attacks, coupled with targeted training, foster a security-focused culture, reducing the risk of actual phishing attacks.

2.2.2 Tailoring Training Programs

Effective training programs must be tailored to an organization's specific needs. This includes identifying common phishing attack types, creating targeted materials, and offering ongoing support. Tailoring training programs is crucial, using simulated attacks to identify weaknesses and address them accordingly.

Topics covered in training may include email security, social engineering, and safe browsing practices delivered through videos, articles, simulations, or classroom sessions. Training should align with employees' requirements, prioritizing sensitive data protection when necessary. Training programs should be continuous and regularly updated to stay up to date, reflecting the latest phishing trends. Ongoing training enhances knowledge retention and practical application.

Tailored training and continuous investment foster a security culture, mitigating the risk of falling victim to phishing attacks. B Organizations prioritize employee training and establish a robust defense against potential financial and reputational harm resulting from successful attacks.

2.2.3 Engaging Employees

Engaging employees in anti-phishing measures is crucial for their effectiveness. This can be achieved through interactive and gamified training programs. Gamification involves turning training into a game-like experience, where employees earn points and rewards for completing modules and competing with peers. By conducting a comparison between games and reading phishing tutorials, the author determined that phishing games offer a more effective method for educating individuals on combating phishing and other security attacks [30]. Leadership involvement is essential, as employees are more likely to take training seriously when leaders demonstrate the importance of security and actively participate. Engaging employees fosters a sense of ownership and increases the likelihood of retaining and applying the learned information in real-world situations.

2.2.4 Monitoring Feedback

Organizations should monitor and provide feedback to employees regarding their performance in detecting and avoiding phishing attacks. This includes immediate feedback on simulated attacks or utilizing analytics to track employee behavior over time. In order to deliver an effective learning experience to learners, feedback plays a fundamental role. Real-time feedback is readily available in lecture-based delivery methods, where the active presence of the instructor during the training facilitates this process [31].

Monitoring and feedback are vital aspects of anti-phishing strategies. Organizations must monitor the efficacy of training programs and simulated attacks to be effective offering feedback to reinforce positive behavior and address weaknesses. Tracking the results of simulated attacks allows the identification of employees or departments needing additional training or support. Employees who report suspicious emails or exhibit cautious behavior should be acknowledged and rewarded. Conversely, employees who fall for simulated attacks or engage in risky actions should receive constructive and supportive feedback, accompanied by further training to reinforce best practices.

2.2.5 Management buy-in

Management buy-in is an essential component of anti-phishing methodologies. When senior leaders within an organization are committed to the program's success, they can provide the necessary resources and support to ensure that the program is effective and sustainable. When leaders understand the potential impact on the organization's reputation, financial resources, and sensitive data, they are more likely to prioritize the implementation of an anti-phishing program. Another way to obtain management buy-in is to demonstrate the program's return on investment (ROI). By tracking the results of simulated phishing attacks and measuring the reduction in risk over time, organizations can demonstrate the program's financial benefits. This can include avoiding financial losses, minimizing remediation costs, and reducing the risk of legal and regulatory penalties.

2.2.6 Comparative Table

The comparison of previous studies is given below in the table:

References	Approach	Methodology	Limitations
[22]	Focused on combined phishing awareness campaigns that comprise simulated phishing attacks and embedded content-based phishing education.	They used operant conditioning theory to improve end-user awareness.	• Sending phishing emails and providing email message-based training to users. • Lacking in video-based interactive content and user awareness evaluations.
[27]	Worked on human factors of phishing and their awareness approach. Their approach was to set	They used the ANOVA approach to evaluate the training effect.	• This approach needs to educate the employee on the core level.

	participants' email client warnings so that they can act proactively on the emails.		• If the email client policy will not work, then there is no awareness in end-users against phishing attacks.
[23]	Performed the phishing simulations and trained the victims by e-learning content-based material	Cyber Drills and Knowledge Transfer	• It only provides CBI awareness and is difficult to understand for end-users because this needs end-user competencies to understand the content correctly. • This content does not provide the simulated awareness templates. • No Interactive evaluation can be performed after the CBI-based awareness.
[25]	The author calculated and compared the effectiveness of three awareness delivery models.	The effectiveness was measured using the correctness percentage (click rate).	• This only explains and compares the most effective training model but not pointing the type of content which can

	The delivery models are Text-based, Game-based, and Web-based training models		provide a more effective impact on security awareness and culture.
[26]	Ran the simulations in groups. The users who clicked on the malicious link show different notifications based on their groups.	They used the ANOVA approach to evaluate the training effect.	• They are not just providing video-based training. • Not evaluating the user by providing interactive games. • Not calculating the Phish-prone percentage for users and organizations.
[24]	Developed and implemented a technical approach in the form of a tool named PhishTester to automate testing whether a website is phishing or legitimate.	They used FSM (Finite state machines) based model.	• Technical tools can protect a user from falling prey to phishing attacks to a certain extent, the user mustn't become too reliant on technology. Thus, it is critical to combine technical tools with phishing training

Table 2.1. Previous Study Comparison

2.3 Summary

Reducing phish-prone behavior is a critical challenge facing organizations today. Phishing attacks are becoming increasingly sophisticated and difficult to detect and can lead to a range of negative consequences including financial losses, data breaches, and reputational damage. To address this challenge, organizations can use various approaches, including conducting simulated phishing attacks, tailoring training programs to individual employees, engaging employees in the program, monitoring and providing feedback, and obtaining management buy-in and support.

Simulated phishing attacks are designed to provide employees with realistic training that mimics real-world phishing attacks. While this approach can effectively increase employee awareness and vigilance, it may also create a sense of distrust and lower employee morale. Tailored training programs can be customized to the needs and preferences of individual employees, but may not be effective for all employees, particularly those who are resistant to change. Employee engagement is critical to the success of any anti-phishing program but requires significant resources and time to maintain engagement. Monitoring and feedback can help provide ongoing assessment of program effectiveness and areas for improvement but can be resource-intensive and may require dedicated personnel. Finally, management buy-in can provide necessary resources and support for the program but may be difficult to obtain without a strong business case and demonstration of ROI.

By combining these different organizations can create a comprehensive defense against phishing attacks. This can involve creating a culture of security within the organization, providing ongoing training and reinforcement, and using data-driven approaches to monitor and improve the program over time. By taking a proactive and comprehensive approach to reduce phish-prone reducing or, organizations can better protect themselves against the growing threat of phishing attacks.

Chapter 3

Proposed Methodology

3.1 Introduction

In this chapter, we are presenting a phishing simulation and awareness tool. Currently, the organizations that are using anti-phishing tools, needs a lot administration efforts, Phishing simulations often fail to replicate real-world phishing techniques, many awareness programs focus on one-time training sessions without ongoing reinforcement or interactive elements, resulting in decreased employee engagement and retention of knowledge and the effectiveness of phishing simulations and awareness programs is often measured solely based on click rates, neglecting other crucial factors such as reporting incidents, identifying sophisticated attacks, and promoting a culture of vigilance. Based on above discussion, we proposed tool which is filling all the gaps and provides effective solutions to organizations.

3.2 Models implemented in Proposed Tool

Phishing is a big business for the cybercriminal. Organizations is to evaluate and choose the best simulation tool which provides real benign simulated attacks, market level trainings through videos, HTML templates, and calculate the phish-prone percentage for organization. We analyzed a lot of tools for the phishing attack simulation and security awareness training for organizations. But the currently available tools are not addressing the needs of the organizations. We performed the analysis and fills all the gaps and address all the organization needs. In proposed tool, not only eliminate the administration efforts, all address the current attacks, phishing techniques and also provides the most effective way to train and track the process of security awareness of the end users.

Developing a phishing tool that incorporates Cialdini's principles of persuasion can be a sensitive topic as it raises ethical concerns. It's important to note that the principles of persuasion should be used responsibly and with proper consent from participants. It's crucial to approach the development of a phishing tool with ethical considerations in mind. The primary goal of proposed tool is to raise awareness, educate individuals

about phishing risks, and reinforce best practices for identifying and avoiding phishing attacks. Proper consent, transparency, and responsible use of persuasion techniques are essential to ensure ethical behavior in the development and deployment of such tools.

In evaluation and awareness, we used CyberDrill. Cyber drills are a valuable tool for evaluating the effectiveness of phishing simulations in an organization. This abstract explores the concept of using cyber drills to assess the impact and response of employees to simulated phishing attacks. The abstract highlights the objectives, methodology, and benefits of conducting cyber drills specifically for evaluating phishing simulations. It emphasizes the importance of creating realistic scenarios, measuring employee response and awareness, and analyzing the results to identify areas for improvement. By conducting cyber drills focused on phishing simulations, organizations can gauge the level of preparedness, identify weaknesses in employee behavior, and implement targeted training and awareness programs to strengthen the organization's resilience against real-world phishing threats.

3.2.1 Cialdini and 6 principles of persuasion

The Cialdini and 6 principles of persuasion refer to the work of social psychologist Robert Cialdini, who identified six fundamental principles that influence human behavior. These principles have been widely studied and applied in various fields. The Cialdini's six principles of persuasion can indeed be applied in phishing simulations to make them more effective in raising awareness and improving security practices. Gabriel and Mohamed (2011) suggest that by gaining an understanding of the factors that influence employee behavior, organizations can effectively decrease or alleviate internal threats [7]. In proposed tool, we designed the email payloads on this principle to create the urgency, curiosity and influence on the end user so that they can phish and in training we also implement this principle to design the games so that user can interact and trained by its influence. Here's how these principles can be utilized:

- **Reciprocity**: In a phishing simulation, you can provide participants with valuable resources, such as educational materials or training modules, before engaging them in the simulation. By giving them something useful upfront, you create a sense of reciprocity and increase their willingness to engage and learn from the simulation.

- **Commitment and Consistency**: Encourage participants to make a commitment to security practices or awareness before the simulation. For example, you can have them sign a pledge to be vigilant against phishing attacks. Once they commit to this, they are more likely to follow through and apply what they've learned during the simulation.
- **Social Proof**: Incorporate social proof into the phishing simulation by sharing statistics or real-life examples of the impact of phishing attacks. Highlight how many people have fallen victim to phishing and emphasize the importance of being cautious. This can create a sense of social influence and motivate participants to be more alert.
- **Authority**: Present the phishing simulation as coming from a trusted source, such as the IT department or a recognized security expert. By leveraging authority, participants are more likely to perceive the simulation as legitimate and take it seriously.
- **Liking**: Personalize the phishing simulation to make it relatable to the participants. Use familiar language, references to their work environment, or even include their names in the simulated phishing messages. This establishes a sense of familiarity and likability, making the simulation more engaging and impactful.
- **Scarcity**: Create a sense of scarcity or urgency around the phishing simulation. For example, you can mention that participation is limited or that the simulation is available for a limited time. This can increase participants' motivation to engage promptly and take the simulation seriously.

By incorporating these principles into phishing simulations, you can enhance their effectiveness in capturing participants' attention, fostering engagement, and ultimately improving their ability to recognize and respond to phishing attempts in real-world scenarios. Psychosocial techniques aimed at manipulating victims, such as assuming authoritative roles or exploiting curiosity, can be employed [11]. However, it is crucial to ensure that the simulations are conducted ethically and with clear communication about their purpose and intent to maintain trust within the organization.

3.2.2 Cyber Drill or Cyber security Drill Methodology

A cyber drill is a simulated exercise designed to evaluate and enhance an organization's preparedness against cyber threats [19]. It involves creating and executing realistic scenarios that mimic potential cyber-attacks to assess the effectiveness of an organization's cyber security measures and response capabilities. Participants, including IT professionals, security teams, and key stakeholders, engage in the exercise to test their ability to detect, respond to, and recover from cyber incidents.

Implementing a cyber-drill in phishing simulations can provide a comprehensive evaluation of an organization's preparedness and response capabilities against phishing attacks. Here's how you can incorporate a cyber-drill into your phishing simulation implementation:

- **Planning**: Define the objectives of the cyber drill, such as assessing employee awareness, response effectiveness, or identifying areas for improvement in phishing awareness and incident response. Determine the scope, timeline, and participants involved in the drill.
- **Scenario Development:** Design realistic phishing scenarios that replicate common tactics used by attackers. Craft phishing emails or messages that mimic the techniques of impersonating authority figures, exploiting curiosity, or leveraging social engineering. Ensure the scenarios align with the organization's industry, employee roles, and responsibilities.
- **Simulation Execution:** Execute the phishing simulation by sending the simulated phishing emails or messages to targeted employees. Monitor their responses and track their actions, such as clicking on suspicious links, providing sensitive information, or reporting the incidents.
- **Data Collection and Analysis**: Collect relevant data throughout the simulation, including response rates, click rates, reported incidents, and employee feedback. Analyze the data to evaluate the effectiveness of the phishing simulations and identify areas for improvement in employee awareness, training, or technical controls.
- **Debriefing and Learning:** Conduct a debriefing session with participants and stakeholders to discuss the results and findings of the cyber drill. Share insights, lessons learned, and best practices to raise awareness and enhance phishing

awareness and response capabilities. Provide targeted training or resources to address identified weaknesses or knowledge gaps.

- **Continuous Improvement:** Use the feedback and insights gained from the cyber drill to refine future phishing simulations and improve overall security awareness. Regularly conduct cyber drills to reinforce training, assess progress, and stay updated on emerging phishing techniques and trends.

By integrating a cyber drill into phishing simulations, organizations can evaluate their employees' responses to phishing attacks, identify areas for improvement, and enhance their overall phishing awareness and incident response capabilities [19]. This iterative approach helps in continuously strengthening the organization's defenses against phishing threats and reducing the risk of successful attacks.

3.3 Flowcharts

This flow of proposed tool evaluation is consisting of three process which are below:

3.2.1 Create Simulation Flow

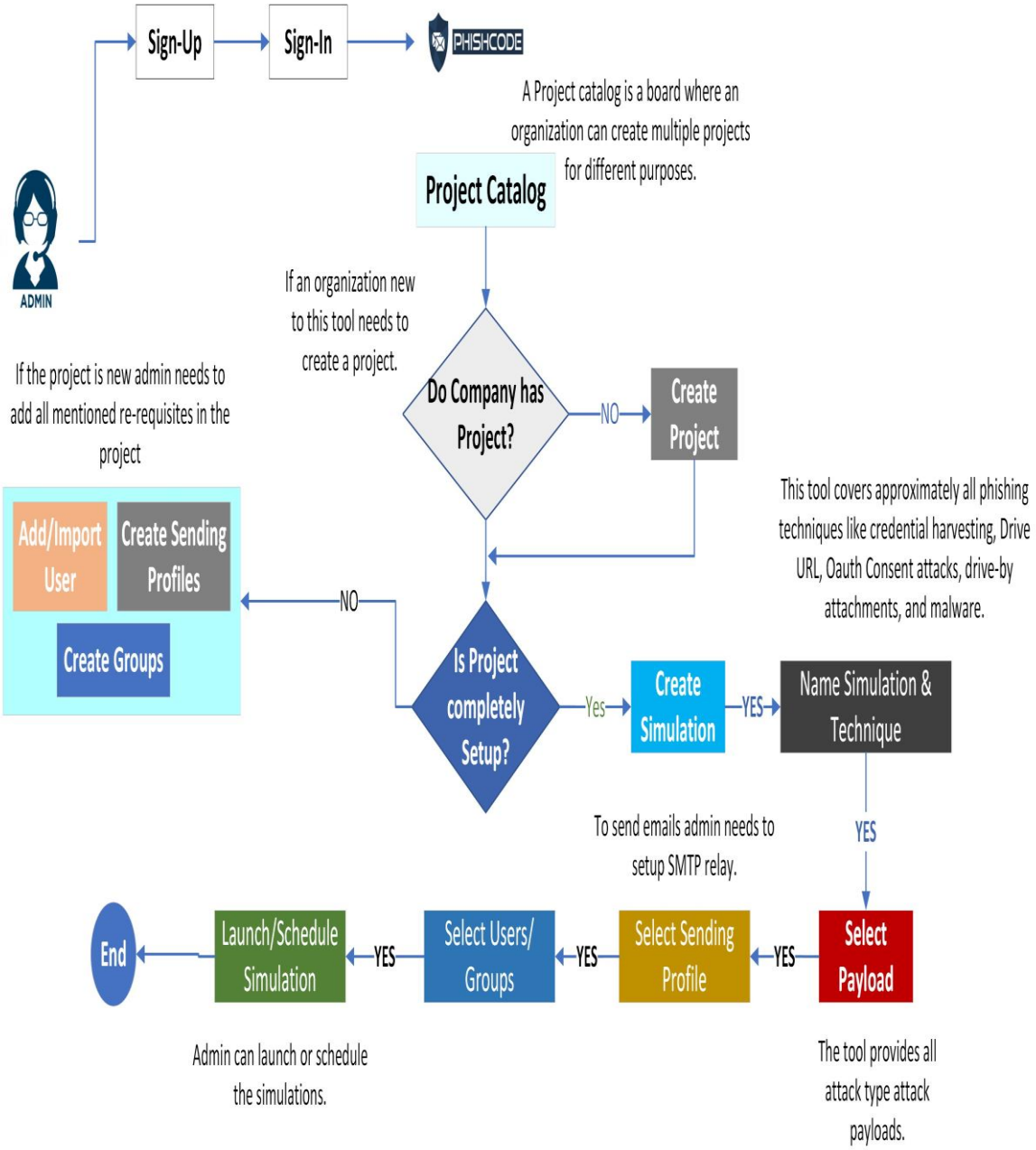

Figure 3.1. Create Simulation Flow

3.2.2 Launch Simulation Flow

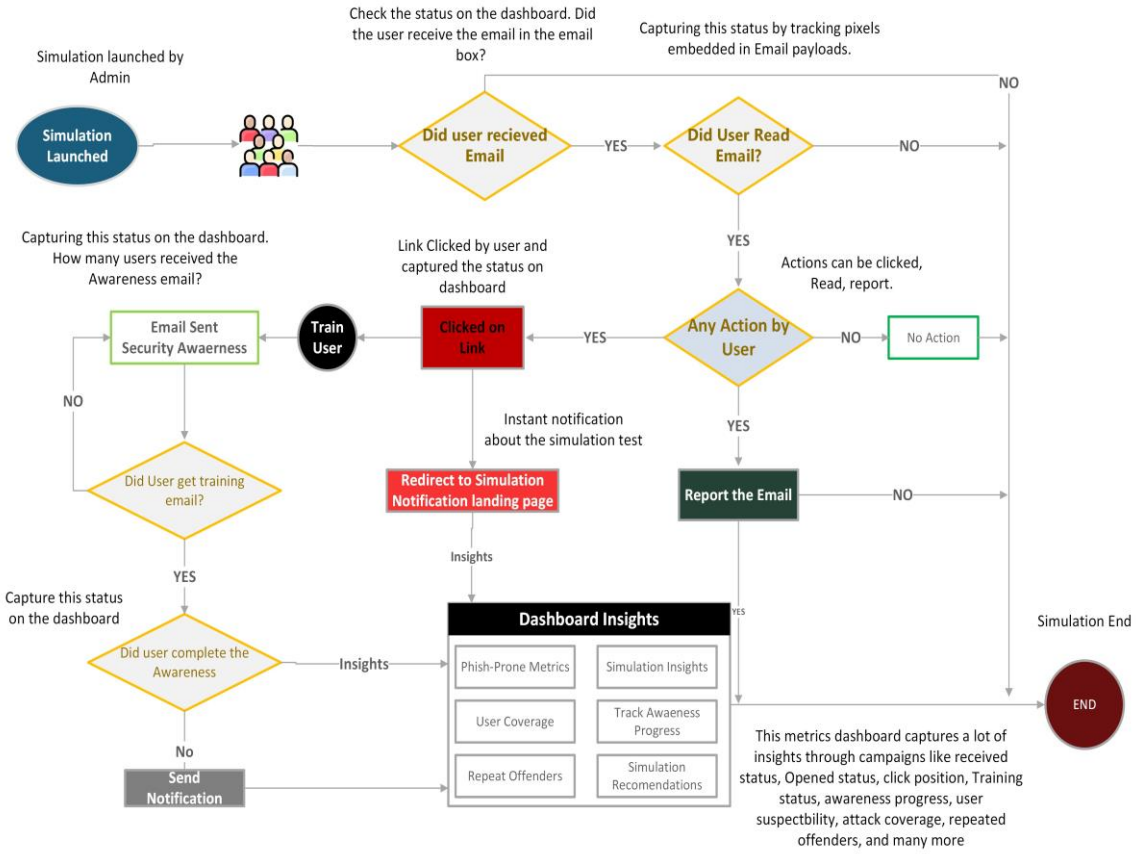

Figure 3.2. Launch Simulation Flow

3.2.3 Security Awareness Training Flow

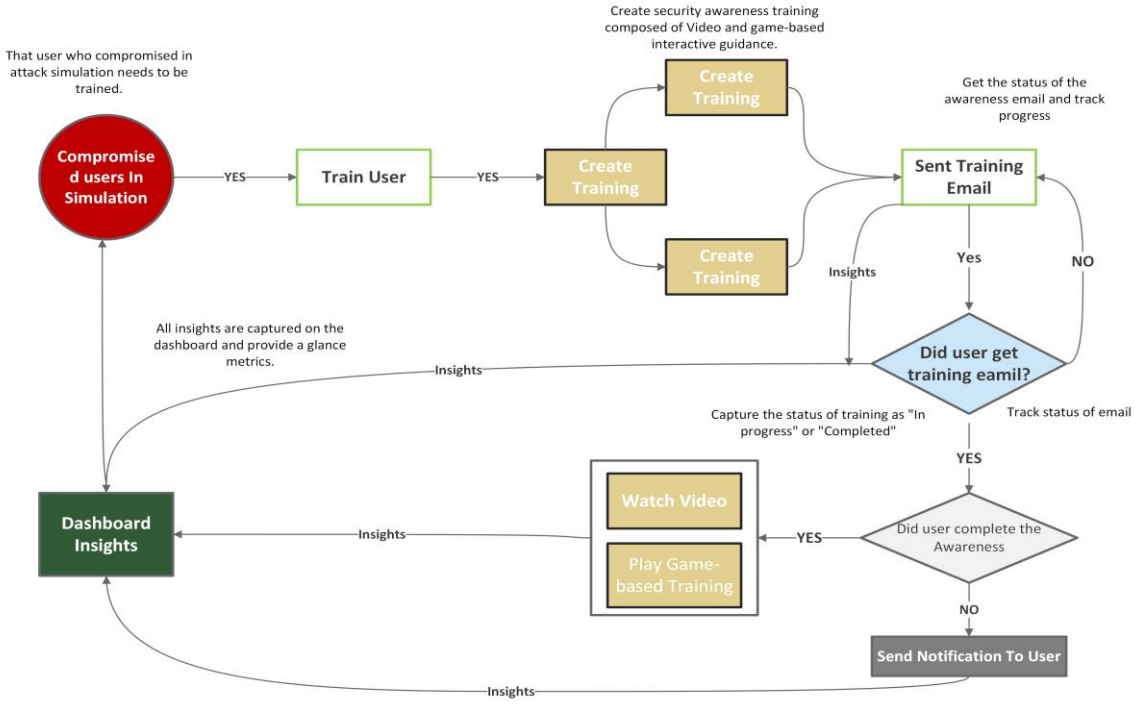

Figure 3.3. Training Flow

This phishing simulation tool is a SaaS application. In the definition provided by Gartner [28], Software as a Service (SaaS) is described as software that is remotely owned, delivered, and managed by one or more providers. The user needs to sign-in into the tool. This tool provides the multi-tenancy/MSSP account management. The administrator needs to create a project (company) within the tool. Import/add the users in the project and the sending profiles (Which send emails to users).

Initial Setup and Create Simulation

- **Signup**

  The user needs to create the account in the proposed solution before starting. The user will add as "Global Administrator."

- **Project Catalog**
  - The admin needs to create the project if the project is already not created.
  - The admin can edit the project on this page.
  - The admin can add new admins in the project and grant them fine grained role base access.
- **Project Setup**
  - The admin needs to add the users or import the user directly from CSV file.
  - Add users in different groups as per their role or department.
  - Add the sending profile which helps admin to send out the emails to the user for simulation.
- **Sending Profiles**
  - Offers pre-built email templates for various social engineering attacks.
  - Allows customization of email content and design to suit your requirements.
  - Provides a range of options for creating persuasive and realistic phishing emails.
  - Allows future customization to create unique and tailored payloads.

- **Email Payloads**
  - This contains the benign real world attack scenarios.

- This section covers most phishing attack techniques like credential harvesting, drive-by-URL, drive-by-attachment, Oaths Consent.

- **Create/run the Simulation.**

  In this phase, the administrator will create a simulation campaign.

  - In first step name the campaign and select the attack technique like credential harvesting, drive-by-URL, drive-by-attachment, Oaths Consent.
  - Then select the payload which want to execute. In this tab you will only be able to those payloads which related to selected attack techniques previously.
  - Also select the targeted user/groups on which want to execute the attack.
  - The administrator can run the simulation immediately or also can schedule it.

- **Attack Simulation**
  - Provides a comprehensive list of all launched simulations.
  - Displays the status of each simulation, such as completed or ongoing.
  - Helps in monitoring the progress of phishing campaigns.
  - Allows you to track and analyze the success rate of simulated attacks.

Launched Simulation Flow Metrics

- **Dashboard**

  This provides a centralized overview of campaign results and metrics. Offers insights into user susceptibility, allowing you to identify vulnerable areas. Measures overall risk levels across your entire organization.

  - **Phish-Prone Metrics**

    Phish-prone metrics refer to the measurement and analysis of employee susceptibility to phishing attacks within an organization. These metrics are used to assess the effectiveness of phishing awareness and training programs. Phish-prone metrics typically include metrics such as click rates.

  - **Simulation Attack Coverage**

This shows the attack simulation coverage on the organization. This provides the percentage of users who face attack simulation vs. who still have not included in any attack.

- **Training Completion**

  This shows the progress of training of compromised users. This has two status “Completed” and “In-progress”.

- **Repeat offenders.**

  This shows the users who compromised in at least in two attacks. They are compromised more than once and needs awareness.

- **Current Launched Simulation Metrics Tracking**
  - **Email Sent Status**

    The administrator can also see the email sent status on the tool dashboard. In this phase, the email is in the mailboxes of the targeted users/groups.

  - **Read Email**

    The administrator can also see the email sent status on the tool dashboard. In this phase, the user may or may not be read the email. But this is a condition, if user will not read the email its means user is secure. If the user will read the email it will initiate further actions.

  - **Caught Users (Compromised Users)**

    The administrator can also see the email sent status on the tool dashboard. In this phase, the user may or may not be clicked or provide the information. This action will define by the type of attack run by the administrator. But this is a condition, if the user will not click/provided any critical information means the user is secure not need to perform any further actions. If the user clicked/provided the critical information, then this means the user is insecure and needs to move on to the next step.

  - **Warning notification**

    When the end user will click/provided the critical information, the simulation will redirect the user to a new web page showing the warning notification explaining how the user failed in the phishing simulation

attack. No, these users need training to increase their awareness about phishing attacks.

- **Simulated User**

  This metrics provides the count of total users who involved in the attack simulation. Also provides the filter to show compromised and uncompromised users on the dashboard.

- **Training Sent**

  This shows the status of training email sent to those users who compromised in the phishing attack.

- **Training Progress**

  This also provides the awareness progress. This metrics has two status “in progress” and “completed”.

- **Report Email**

  The users who find the email suspicious can report to admin directly by email.

Training Flow Metrics

The users who compromised need to train and enhance their awareness against attacks.

- **Train Users**

  The users who compromised will appear on the dashboard and admin needs to train them to reduce the phish-prone percentage of organization.

- **Select Training**
  - In this pane, the admin will select the appropriate video training to educate the user visually.
  - The admin can also select the phishing game-based training. In this the end-user needs to interactive with email payload to get the betters insights how to find the phishing spots in an email.

- **Training Email Status**

  The tool will show the status of the email which sent to compromised users.

- **Training Progress**

  The status of training can be captured on the dashboard. This feature has two statuses “In progress” and “completed”. The administrator can track their progress. This also must action user did not complete the training or completed the training.

Training Hub:

Offers a dedicated section for security awareness training. Covers a wide range of topics related to security and compliance. Provides interactive and engaging training materials for end users. This provides an innovative approach to security awareness.

- **Game-Based Awareness**

  Phishing game-based awareness programs have emerged as an innovative approach to educating employees about phishing risks. These programs utilize interactive and gamified elements to simulate phishing attacks and provide immediate feedback on user responses. By engaging employees in a fun and competitive environment, these games enhance awareness, encourage active participation, and reinforce best practices for identifying and avoiding phishing threats.

- **Game-Based Awareness**

  Video-based phishing awareness programs offer an engaging and visual approach to educating employees about phishing risks. This program utilize video content to simulate real-life phishing scenarios, demonstrate common tactics used by attackers, and provide guidance on how to identify and respond to phishing attempts. By leveraging visual storytelling and demonstrations, video-based awareness programs aim to effectively communicate the dangers of phishing and equip employees with the knowledge to make informed decisions when encountering suspicious emails or messages.

3.4 Methodology

In this study, attack evaluation consists of two phases. Both phases were performed in 2 weeks' time frame to evaluate phish-prone percentage. We proposed effective ways to train your user and reduced their attack susceptibility by providing them the security awareness in an effective way.

Phase 1: Cyber Drill

In the first phase, the simulation attack was performed on the chose user group. This attack was performed without any prior notification about the campaign. In this simulation attack, the Company X used the "account expiration" template which was sent to 20 students. After the successful completion of the simulation attack, the data was collected from the company.

- **Security Awareness Transfer**

To find the effective way of training which has more positive effect on reducing phish-prone (user susceptibility against phishing attacks), we selected the video and game-based training model. The training is only provided to those users who clicked on the benign malicious URL. The security awareness training was conducted in the following way.

  - The compromised user received the training email. The email has link to video content and also after completing the video the user needs to give evaluation. The user needs to see video before giving test which is a game-based interactive evaluation. The video has interactive content which explains about "How to spot phishing". After completion of video, the user needs to move for game-based training and user needs to interact with an email which has phishing spots and after evaluating the template the user needs to provide their verdict about the legitimacy of the email.

Phase 2: Cyber Drill

In this phase, the company X again conducted the phishing attack simulation just after one week of previous phase. In this simulation, the Company X used a new email payload, this payload is message returned template. This payload creates inquisitiveness in the students to see which messages was returned to server and not delivered to their inboxes. The same 20 users were involved in this attack simulation. After the successful completion of the simulation attack, the data was collected from company X for analysis of this conducted research.

3.5 Proposed Tool Design

The proposed tool is built using a robust and versatile tech stack that combines the power of React.js for the frontend, Spring Boot for the backend, and PostgreSQL for the database. This combination of technologies provides a solid foundation for developing a secure and efficient product.

To store and manage data, proposed tool employs PostgreSQL, a popular and reliable relational database management system. PostgreSQL offers a wide range of features, including high performance, scalability, and data security. It provides a structured

approach to organizing and retrieving data, ensuring data integrity and consistency. PostgreSQL is also highly compatible with various programming languages and frameworks, making it a flexible choice for backend development.

The integration of React.js, Spring Boot, and PostgreSQL in the proposed tool offers numerous benefits. The frontend built with React.js delivers an engaging and user-friendly interface, while the backend powered by Spring Boot ensures a robust and scalable and secure architecture. The combination of these technologies enables real-time data processing, seamless user interactions, and efficient handling of complex business logic. Furthermore, PostgreSQL serves as a reliable and secure data storage solution, enabling the tool to handle large amounts of data with ease.

3.5.1 Proposed Tool Technology Stack

Technology Stack	
Front-End	ReactJS v18
Back-End	Spring boot: 2.3.2
Database	PostgreSQL v15
Development Environment	VS Code v1.75

Table 3.1. Proposed tool Technology Stack

Deployment Server Specifications	
CPU	2 vCores
RAM	4 GB
SSD Storage	160 GB

Table 3.2. Deployment Server Specification

Chapter 4

Experimental Steps and Scenarios

4.1 Introduction

In the previous chapter, we discussed the proposed model and its implementation. In this chapter, we will evaluate and validate the efficiency and accuracy of designed tool. We discuss about the issues or gaps which we identified within the organization X current phishing simulation and awareness program. For tool evaluation/assessment one multi-national organization is selected. The selected organization is asked to provide the organizational information, but we face a bit of hesitancy during this process. The proposed tool is implemented securely to provide the services to the organization.

4.2 Practical Evaluation

For tool evaluation/assessment one multi-national organization is selected. The selected organization is asked to provide the organizational information, but we face a bit of hesitancy during this process. The proposed tool is implemented securely to provide the services to the organization.

4.2.1 Organization Structure

The selected organization for tool assessment is located in Tysons Corner, Virginia, United States. The organization was established in 2019. Initially, it had started to provide the Cybersecurity training but after some time they also launched their MSSP services. The organization's main business line is cyber security boot camps, professional services and MDR services to their global clients in US. The objective of this organization is to provide high-quality cyber security trainings, professional resources and managed detection and response for the clients. The name of the organization is not to be disclosed as per the company’s condition.

Organization Name	Company X
Address	Xxxxxx
Branch Office	Xxxxxx

Your organization main line of business?	CyberSecurity Boot camps and MDR services
No. of staff do you employee?	640
Organization type	LLC
What Security technologies are used?	SIEM, EDR, XDR, Email Security, PT, SOC, CASB, DLP, Compliance
Objectives while Delivering the Services	Defend the attack surface area of organization. Mitigate human and technology risks.

Table 4.1. Organizational Information

4.2.2 Current Workflow of Company X

Before recommending proposed tool to the Company X, we analyzed the current security awareness procedure within their environment. We have used the Microsoft Visio to illustrate the current tool and practices of Company X security awareness capabilities and practices (shown in Figure 4.2 and in Figure 4.3). We have drawn the current model of company X to evaluate the phishing risk and human awareness.

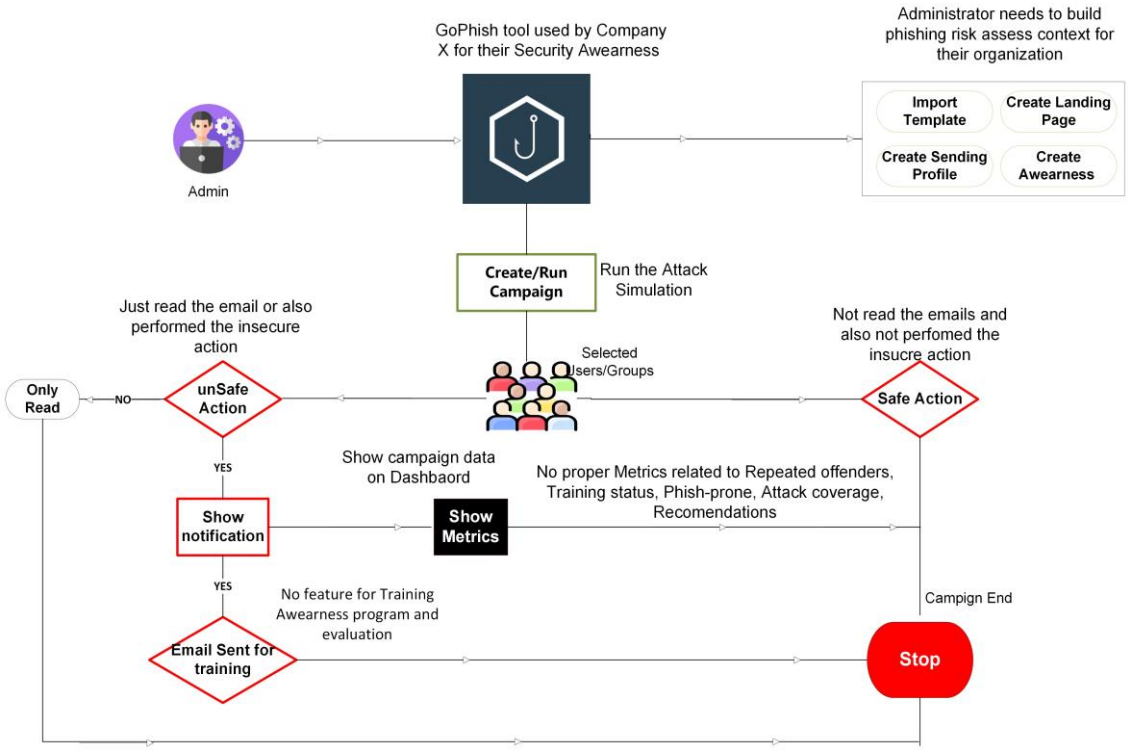

Figure 4.1: Company X Phishing Awareness Model

Company X is using GoPhish tool for the phishing risk analysis. The admin needs to create email payload or import from internet, also need to create or import the landing page. This needs a lot of administration efforts. The admin will run the campaign on the users/groups and track their progress on the limited visibility dashboards.

4.2.3 Gaps Identified in Phishing Awareness Program

In this section, we identified and described the issues in the existing workflow of organization. Based on the identified problems, a new phishing simulation and security awareness tool is proposed to reduce the phish-prone and also track OOTB metrics.

Identified Issue 1:

Currently, Company X is using GoPhish for phishing risk evaluation. In GoPhish, the administrator must create/import the email payloads and landing pages. Technical administration efforts are needed. This also created a security flaw if the admin can use any internet-available template this can also damage the security and consistency of the simulations. After the completion of the simulation, GoPhish provides very limited capabilities in terms of visibility or metrics.

Identified Issue 2:

Also, the organization is not able to evaluate the metrics on organization level. Their current tool does not provide the phish-prone percentage, the progress of security awareness, repeated offenders, and latest real attack templates with OOTB, training game-based template which provides the interactive way of learning. Information Security Awareness Training (ISAT) is commonly suggested as the way to improve user awareness [41–43]. The effectiveness of this program totally depends on the way of delivering.

There is a no way to address following gaps in their model:

- No proper evaluation of phishing risk
- No method to evaluate the organization susceptibility against phishing attacks (Phish-prone)
- Specialized security awareness is not part of their program.
- No track about the training progress of the security awareness.
- No track about the offenders. Those users how repeatedly performing unsecure actions in different campaigns.
- Phishing techniques and attack types of suggestion to improve the phishing risk.

The proposed tools provide accurate metrics to the organization through which organization measure their real phishing risk state and also track the progress which helps organization to measure their security controls and user behaviors.

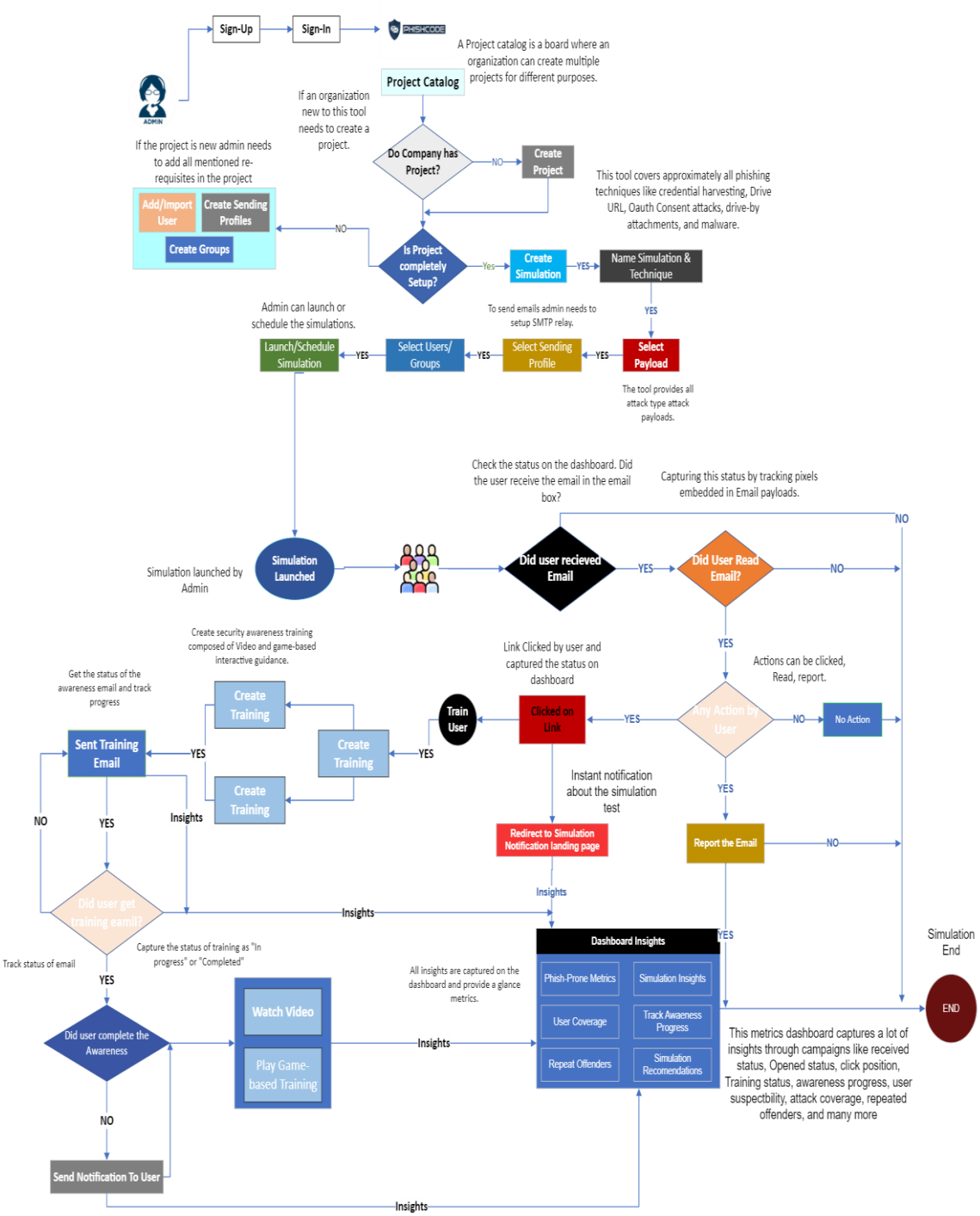

Figure 4.2: Proposed Model for Company X

4.3 Experimental Scenario for Company X

The phishing tool is programmed for this experiment. This is a SaaS based application. Which provides the OOTB (out of the box) real attack simulations, security awareness (Video and HTML templates) and evaluation of the phishing risk (Phish-prone) of the organization. For our research implementation we on boarded the US based well known and leading training institute, which provides the IT and security education and services to their client. We will represent this organization as "Organization X" due to security reasons. We select small group of students for our experiment. We performed two simulated phishing attacks on the organization.

4.3.1 Compliance and Ethical Considerations

- **Ethical Considerations**

  In this experiment, we considered the ethical and social norms of the people included in this experiment. We considered not to override any religious, social norms. Before designing the template, we focused on this and discussed it with organization. Certain ethics committees maintain the belief that it is unethical to deceive individuals for research purposes, prioritizing the well-being of participants over the learning gained from experiments. This approach recognizes the potential psychological harm or distress that participants may experience as a result [32].

- **Data protection and Privacy consideration**

  In this experiment, we launched the "Credential harvest" phishing attacks. In our attack we not capturing or storing any critical information in our database. We are fully compliant with the Organization Privacy and data protection policies. We protect their privacy in terms of their names, emails accounts, passwords, and groups.

- **Selecting Participants and Group Size**

  To conduct the experiment in complete organization is not possible due to the students being at different geographic location. We chose the set of 20 students on which we will perform the phishing attack. This selection was made with the help of the organization point of contact and this will remain the same throughout the experiment.

4.3.2 Creating Phishing Content

- **Email payloads**

  To conduct the experiment, we designed the two templates for the organization. This tool is designed for simulation, that is why we don't have the email payloads. Phishing has different attack techniques, but we used credential harvesting techniques and design payloads. In credential harvesting, the attacker tries to steal critical information like passwords, keys etc. [36]. In this experiment, we are not capturing or storing the credentials into our database as per our contract to the organization. We designed two templates for the students, one is account expiration and second is message quarantined. All the templates were designed using "Cialdini and 6 principles of persuasion", which creates urgency within the students.

  In the first simulation, we used the account expiration template. In this template, we performed the targeted attacks on the user and create the urgency for deleting your accounts within short amount of time. This payload has embedded link of the landing pages, which explains about the benign phishing attack and some information about the attack. Please find below image for your reference:

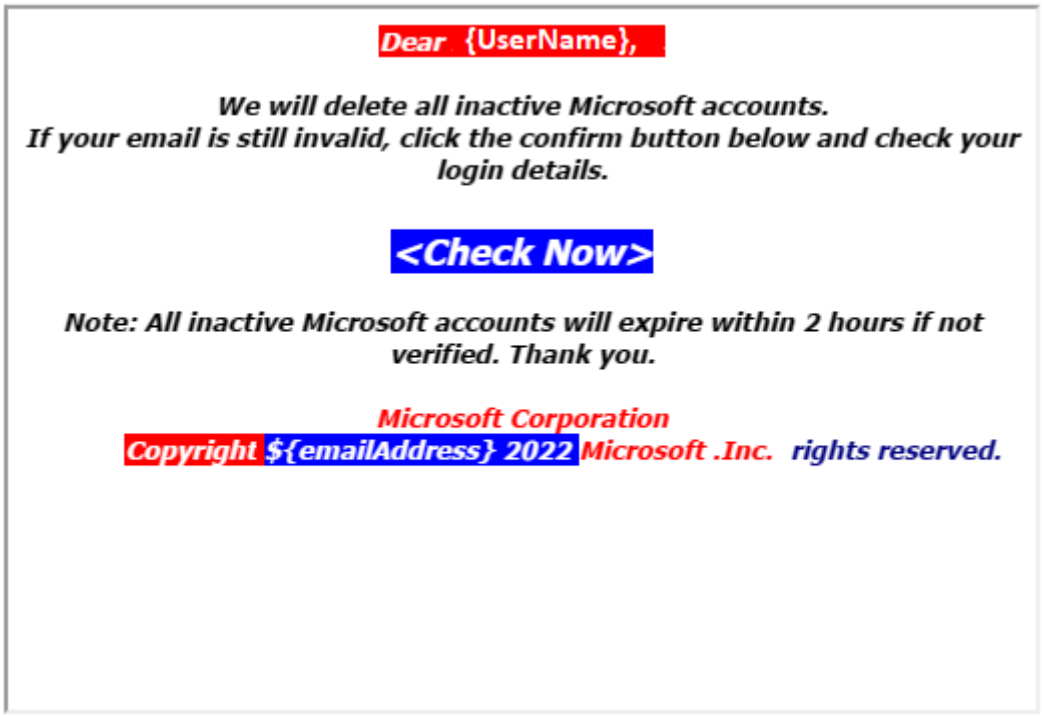

Figure 4.3. Account Expiration Payload

In the second simulation, we used the message returned template, which creates inquisitiveness in the students to see which messages was returned to server and not delivered to their inboxes. This payload has embedded link of the landing pages, which explains about the benign phishing attack and some information about the attack. Please find below image for your reference:

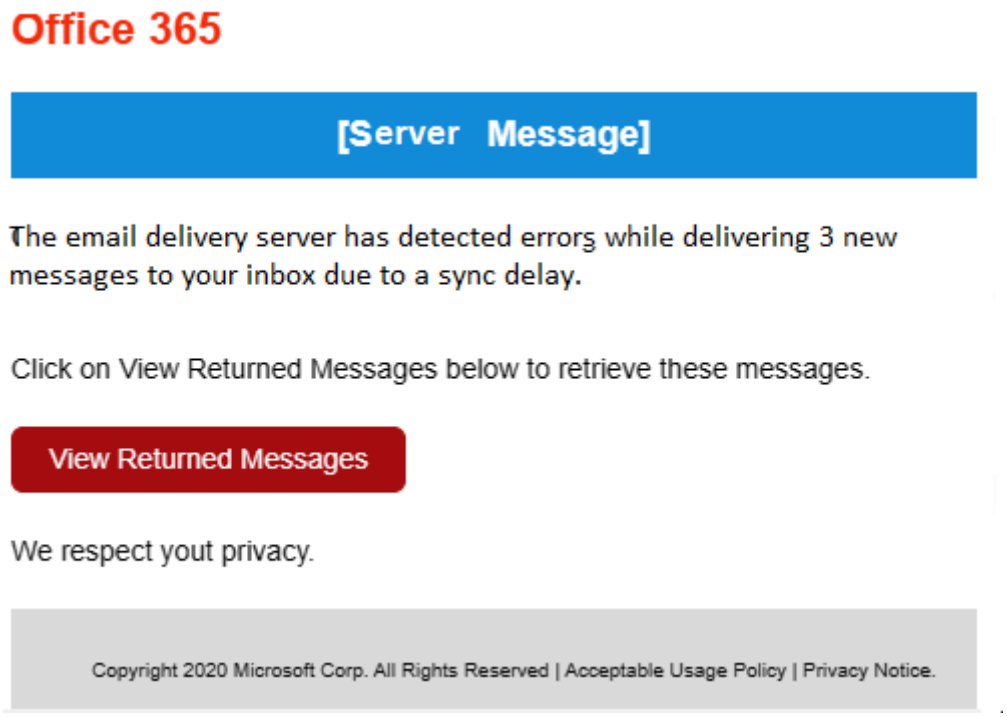

Figure 4.4: Message Returned Payload

- **Landing Page**

  The landing pages divided into multiple categories. We create landing page for instant message about the phishing simulated attack. When the user clicks on the phishing link, it redirects to the page where instant insights are provided to user about the attack. In our landing page, we educate the user about the phishing attacks, and how to report them. Please find below images for your reference:

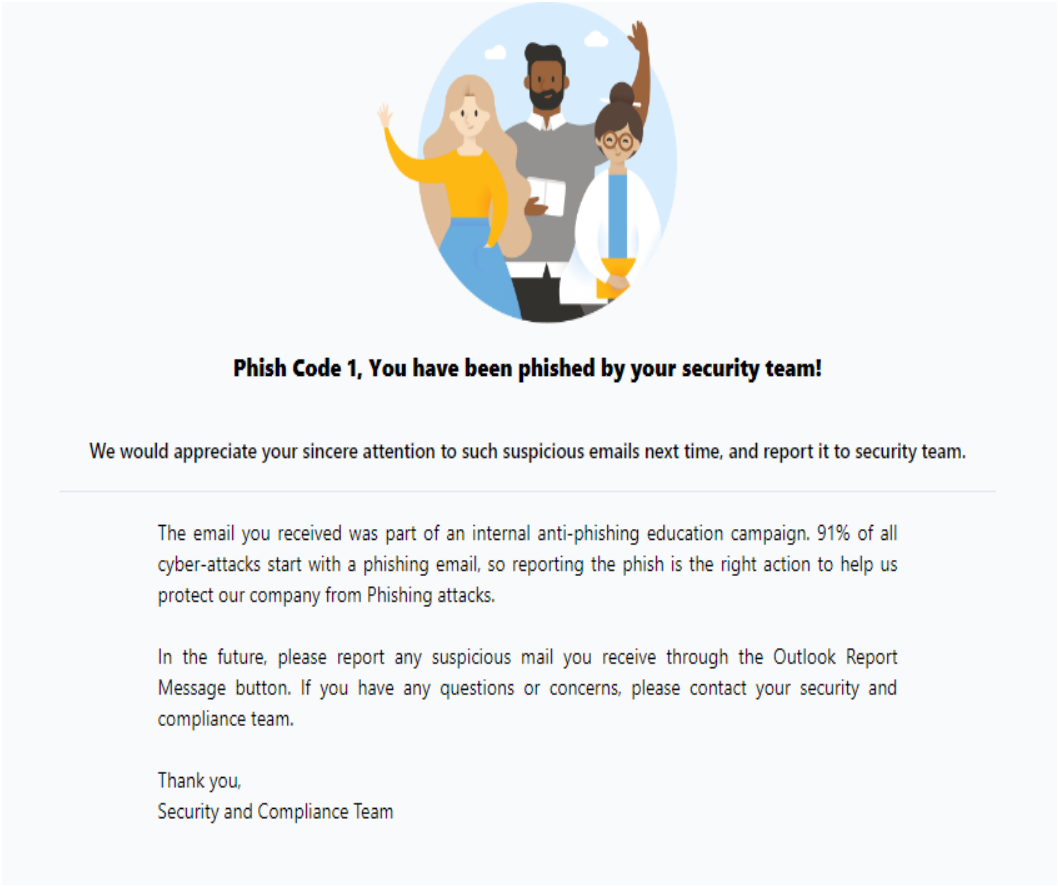

Figure 4.5: Landing Page

4.3.3 Launching Phishing Attack Simulation

Before launching the simulation, the organization needs to create the project. This feature acts as multi-tenancy. Organization X created the project in the tool.

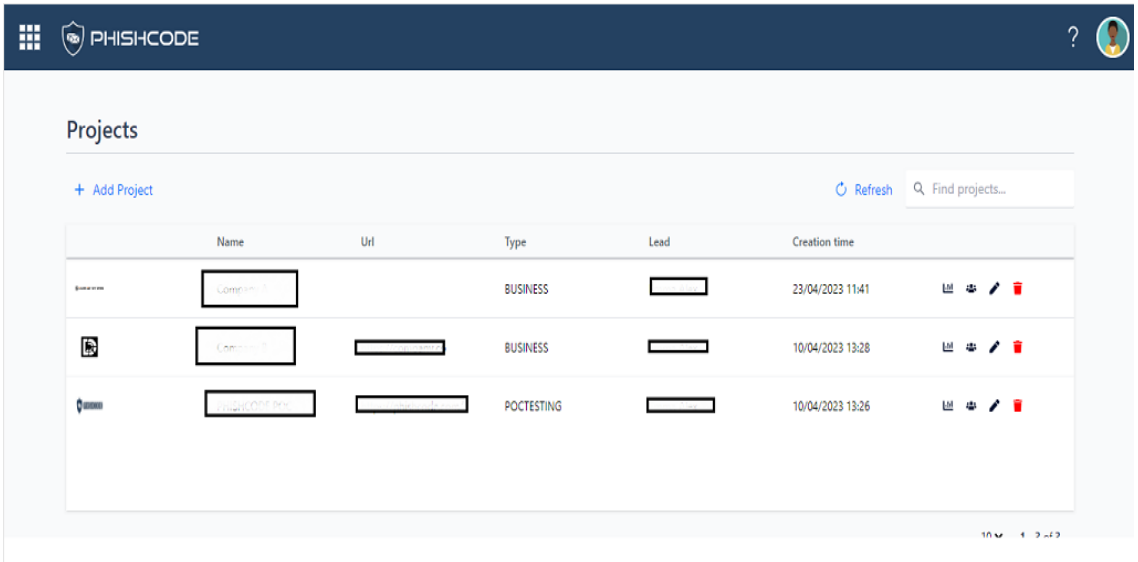

Figure 4.6: Project UI

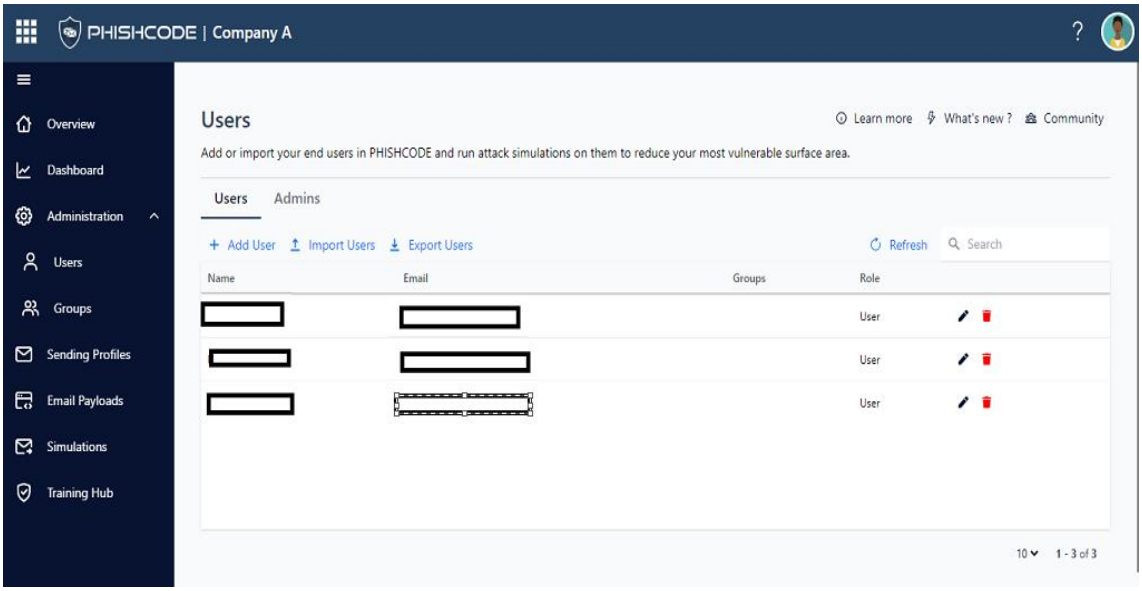

Figure 4.7: User and Group Management

In project they import all the selected students for the experiment purpose. They added their selected buy domain as Sending profiles for testing purposes. We work with their IT admins to whitelist the IP of server and domain through which we want to run the attack.

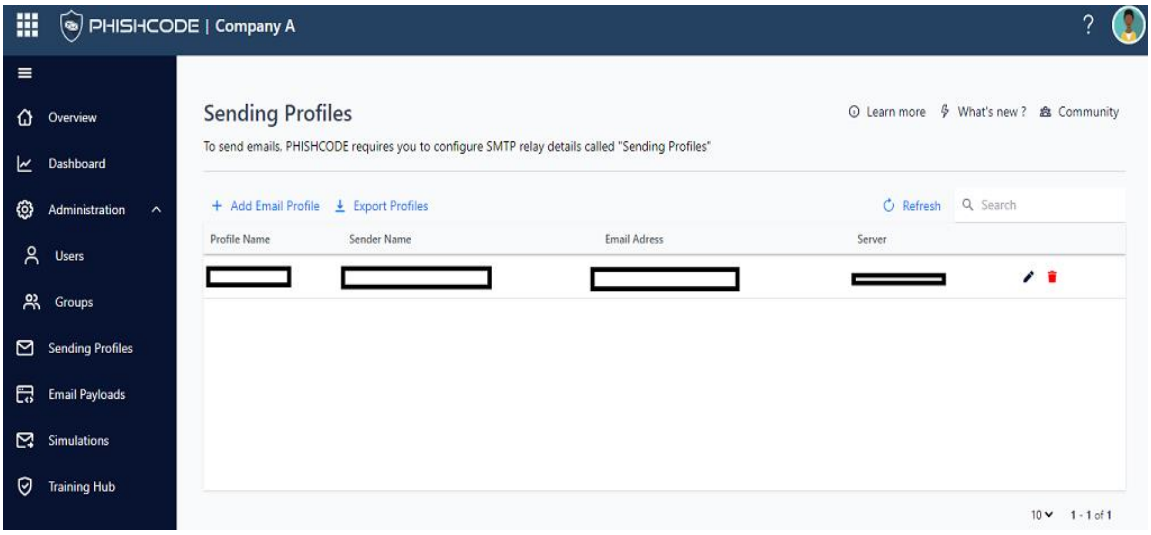

Figure 4.8: Sending Profiles

The tool has the capability to run the attack simulations on the user. The organization launched the simulation on their users through the tool UI. This the pane from where the admin can run the attack simulations. The + Launch Simulation will open a pan to create a simulation. Please find below image for your reference:

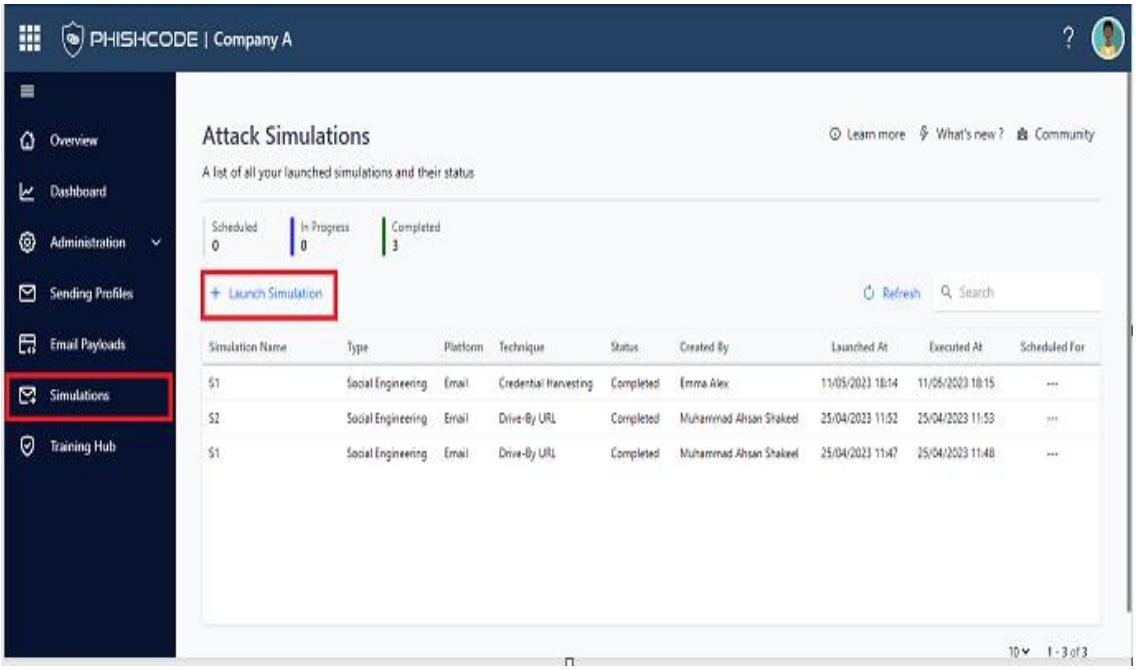

Figure 4.9: Attack Simulation

The admin will provide the name to Simulation and select the technique. In our case, we run simulations on credential harvesting.

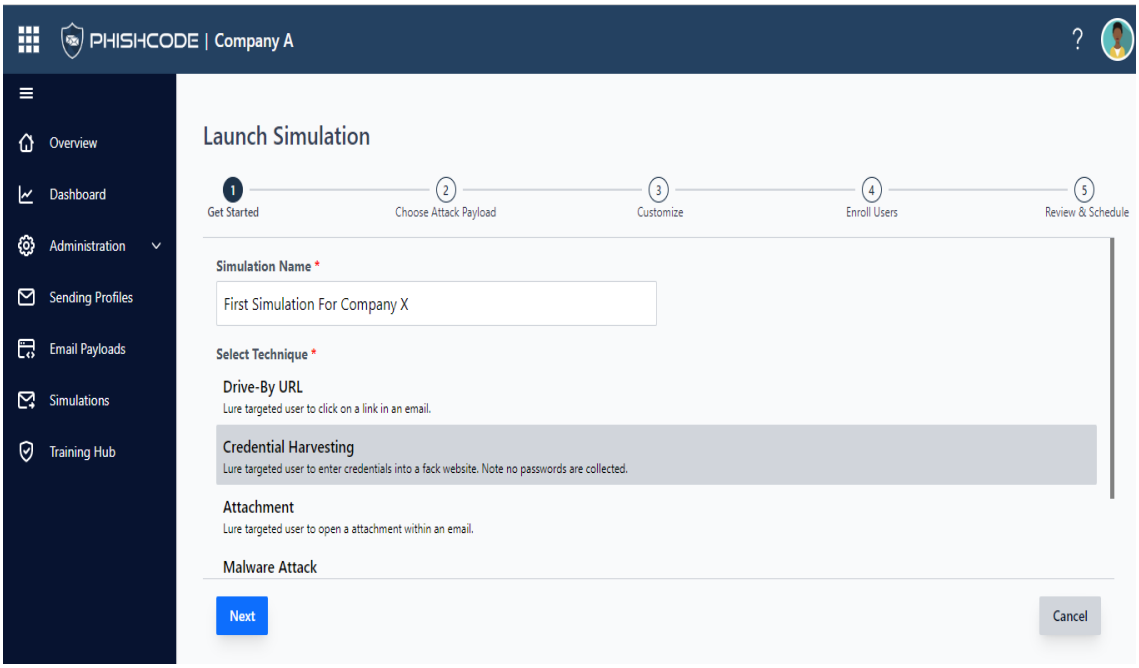

Figure 4.10: Phishing Attack Techniques

In this pane, we selected the "**account deletion**" payload for the first-time simulation.

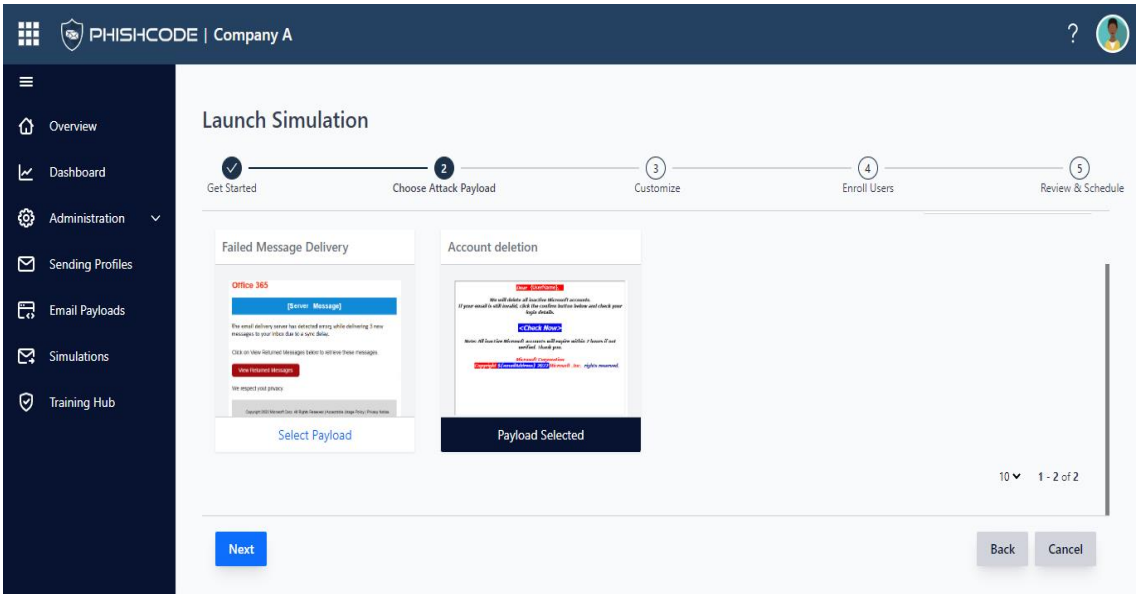

Figure 4.11: Select Email Payload

Select the choose domain through which admin want to run attack their users. We remove data due to security reasons.

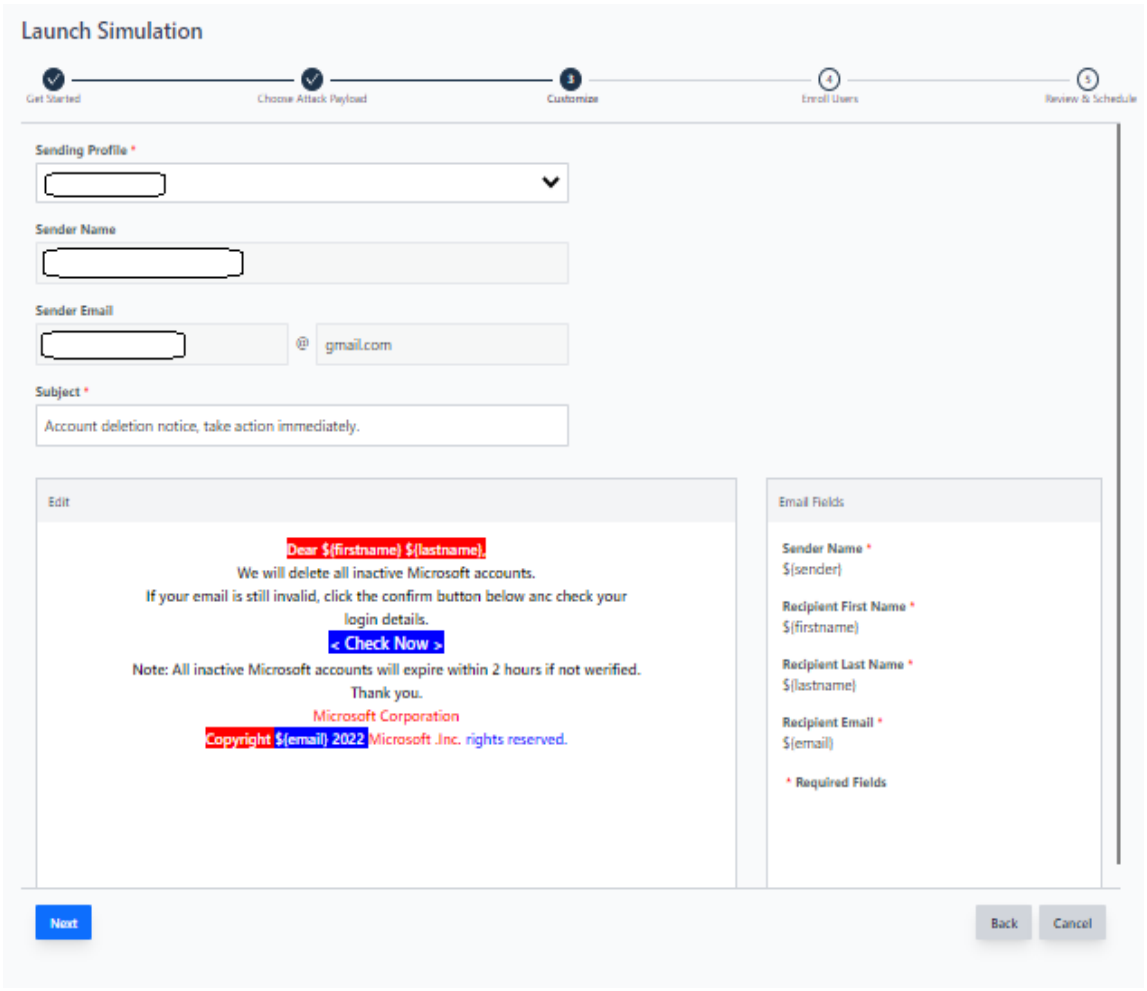

Figure 4.12: Selecting Sending Profiles

The admin will choose all the users which we selected for the phishing testing.

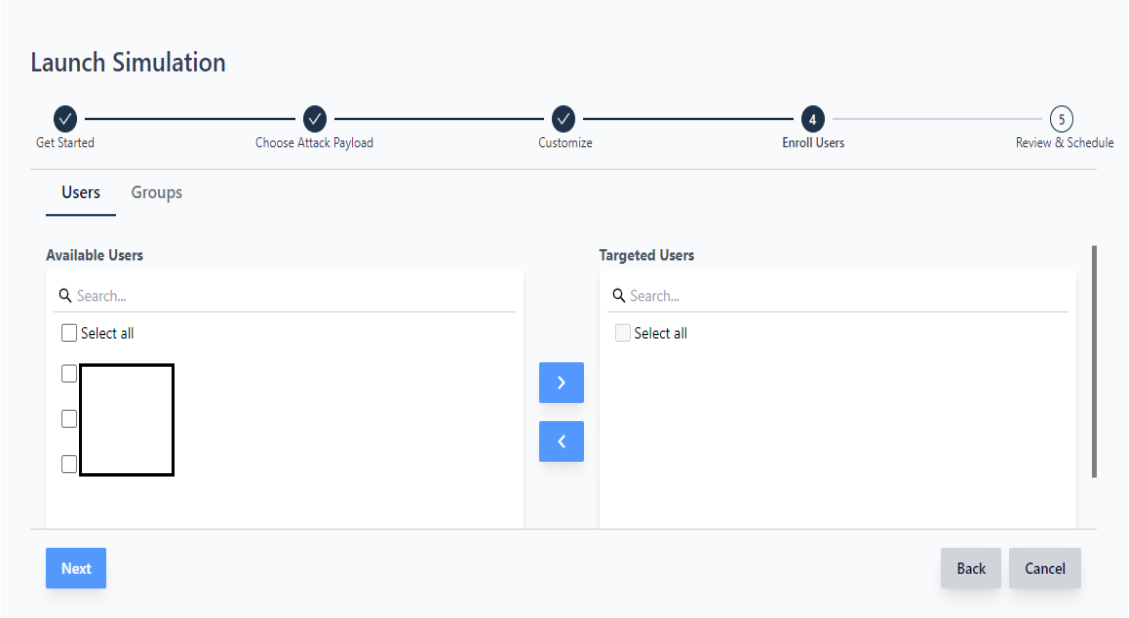

Figure 4.13: Selecting Users and Groups

The admin will run the attack simulation campaign immediately to launch the attack.

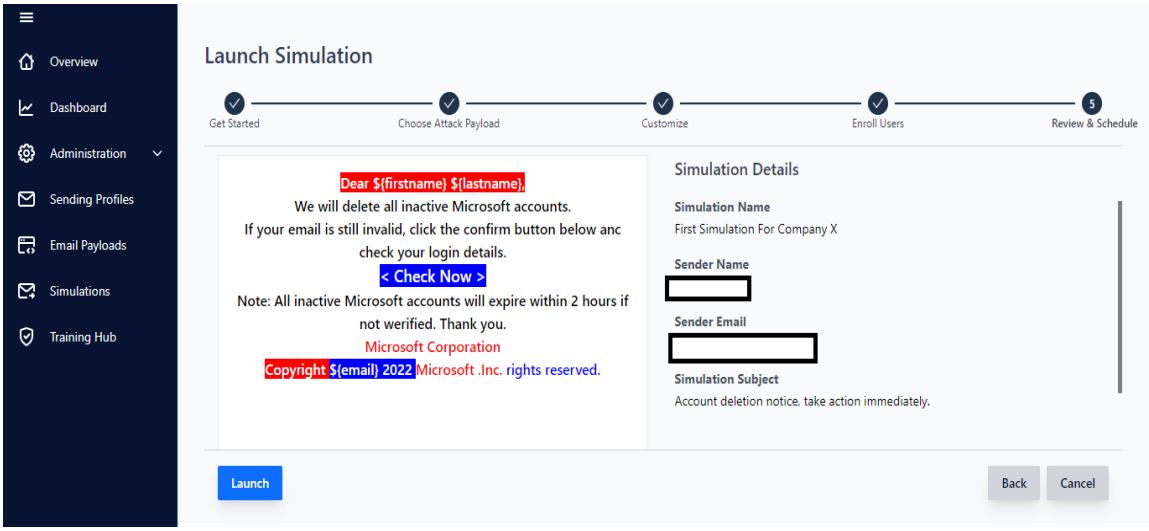

Figure 4.14: Schedule/Launch Simulation

4.3.4 Dashboard and Simulation Metrics

In our tool, we provide at-a-glance metrics for the admin to evaluate the Simulation progress and a lot of other metrics which provide the current accurate phishing risk state and end user's training progress and evaluation.

- **Current Simulation Metrics**

The tool provides OOTB (Out of the Box) visibility against each simulation, which helps organizations to measure their current phishing risk state and user susceptibility (Phish-prone) against attacks.

- **Emails Sent**

  These metrics show the status of sent emails. The status shows the acknowledgment of the server of the sent emails to targeted users. This shows the total number with the percentage. This provides complete visibility against sending emails.

- **Emails Opened**

  This metrics show the status of opened email by targeted user. To track this, we embedded the 1pxel image to our template which hosted on our server. When the user open the email it send the loading request to our server and we captured the state and show it on metrics.

- **Users Caught (Compromised Users)**

  Where template has benign malicious link, when user clicks on URL or button we captured this request and redirects user to our landing page which show instant message about phishing simulation.

- **Users Trained**

  When user click on benign malicious link, we send them the security trainings (Video/HTML based content) and also captured their status and show at here.

  Please find below image for your reference:

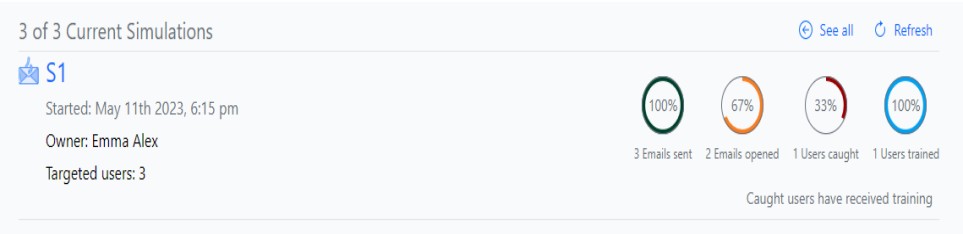

Figure 4.15: Current Simulation insights

- **Simulation Summary Report**

  This pane provides deep insights for selected simulations.

  - **Compromised Users:** The users who clicked on insecure links. This show results in percentage and total number.

- **Uncompromised Users:** The users who did not act insecurely, means did not click on the any malicious links or not download any attachment.
- **Simulated Users:** The user who involved in the attack simulations.
- **Training Status:** Shows the users who received the training emails.
- **Training Completion:** This shows the status about the security training progress who clicked on the malicious links.

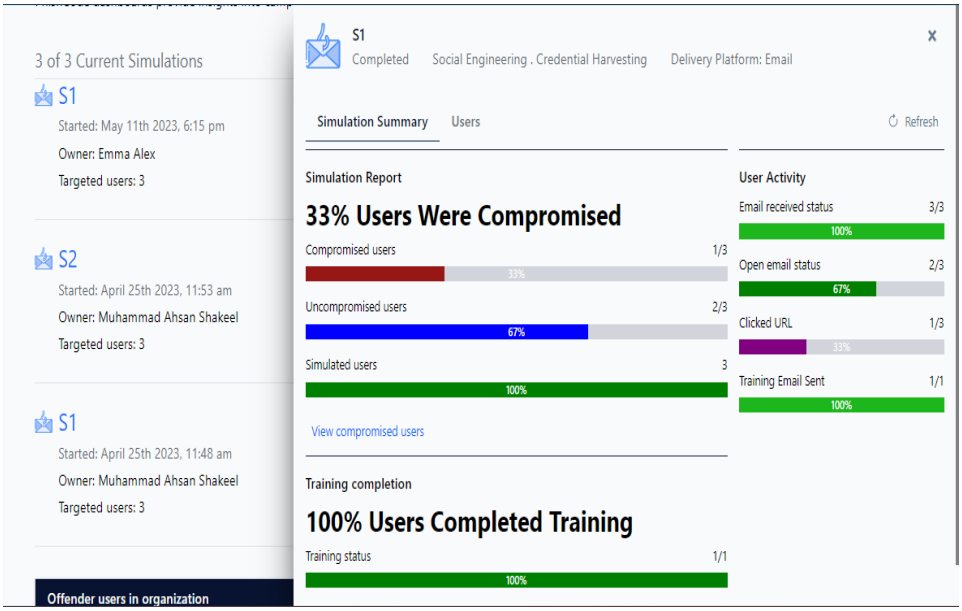

Figure 4.16. Deep Simulation Insights

- **Users Status**

  This report provides deep insights into the simulation. This page has user groups, email sent status, email opened status, and URL clicked status, training status, offender User.

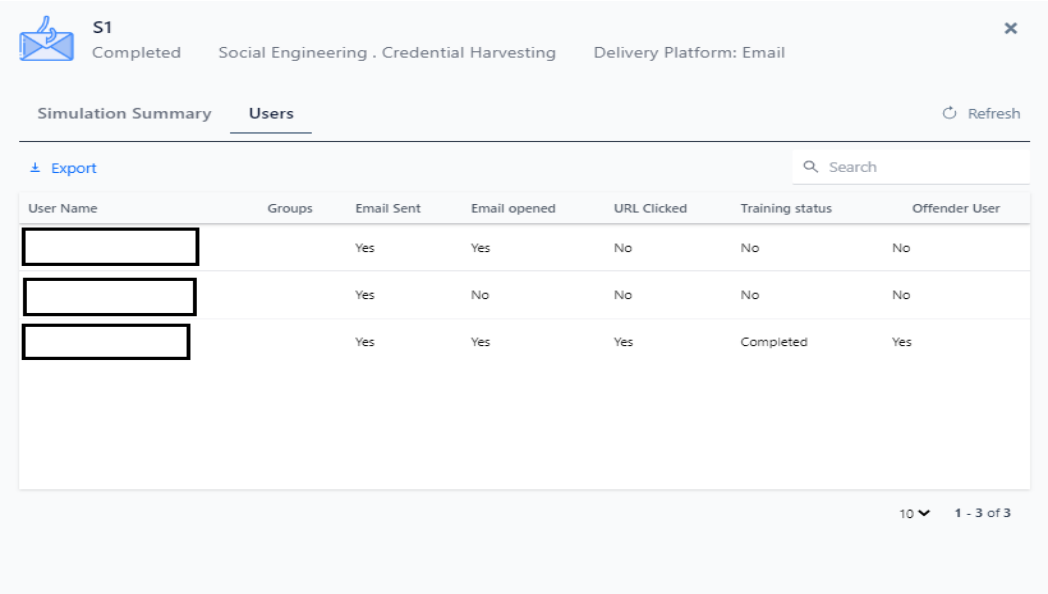

Figure 4.17. Users Insights

4.3.5 Organizational Metrics

The tool provides the OOTB evaluation metrics not only simulation basis but also on the organization level. These metrics provide organizational-level phishing risk, user awareness evaluation, phish-prone percentage and training progress.

- **Offender Users**

  The users who compromised in more than one attack simulations. We track these users against each simulation and also provides the insights about each compromised activity.

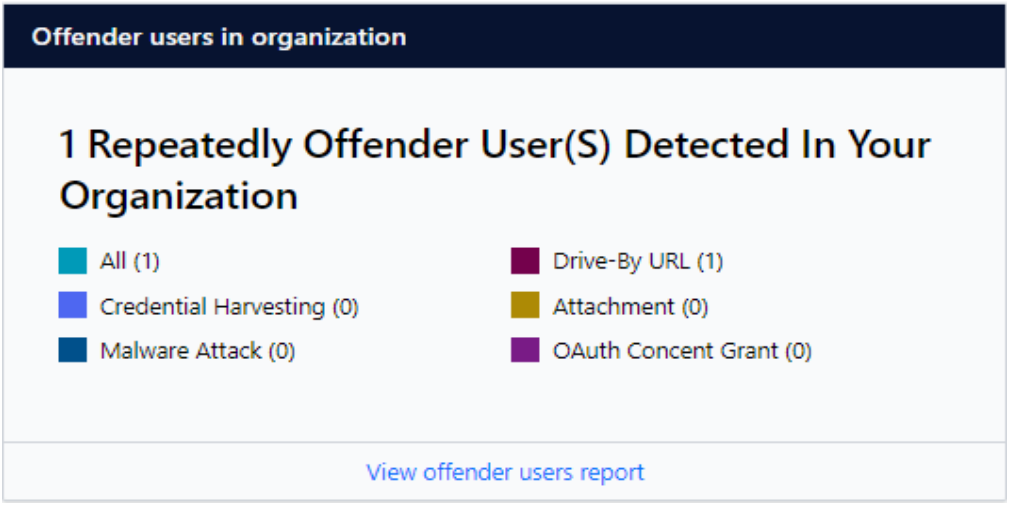

Figure 4.18. Repeat Offenders Metrics

The offender user report provides more insights. This provides the username, repeated count and attack techniques against which they caught.

Figure 4.19. Repeat Offenders Reports

- **Phish-prone Percentage**

Figure 4.20. Phish-Prone Percentage

- **Attack simulation coverage**

  This dashboard shows the count of simulated and un-simulated users of the organization. The metrics also provide visibility in number and percentage.

Figure 4.21: Attack Coverage Metrics

This metrics report provides deep insights about the user coverage like usernames, simulation status, compromised status and Offender status.

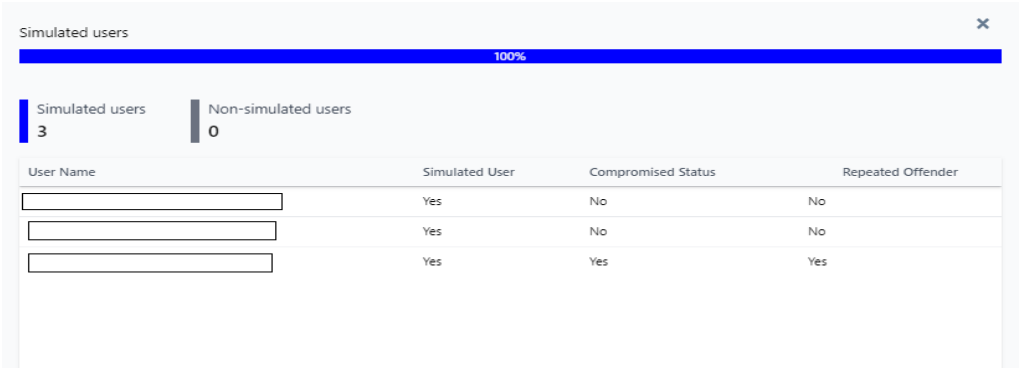

Figure 4.22: Attack Coverage Report

- **Phishing Awareness Training Completion**

  This metrics shows the status of trainings, which sent to those users who compromised in any Simulation attack. This has two statuses **Completed** (Who have seen the video or HTML Template evaluation) and **Pending (not completed the Video or HTML Template evaluation).**

Figure 4.23: Awareness Training Progress Metrics

This report shows the data like usernames who received the training, simulation in which they got caught, simulation type, training name and their status.

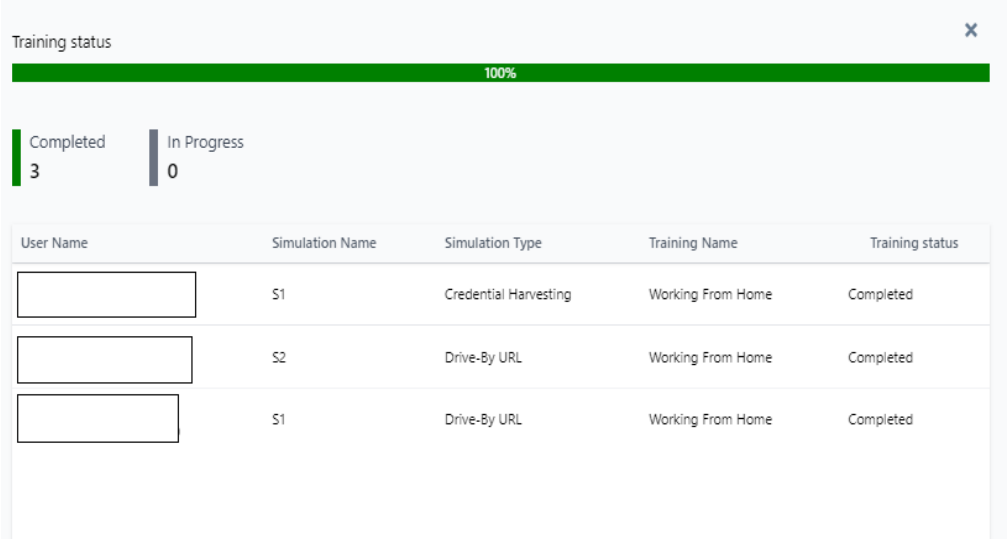

Figure 4.24: Awareness Training Progress Report

- **Simulation Recommendations**

  These are the recommendations which we provide to our customers as per phishing market trends.

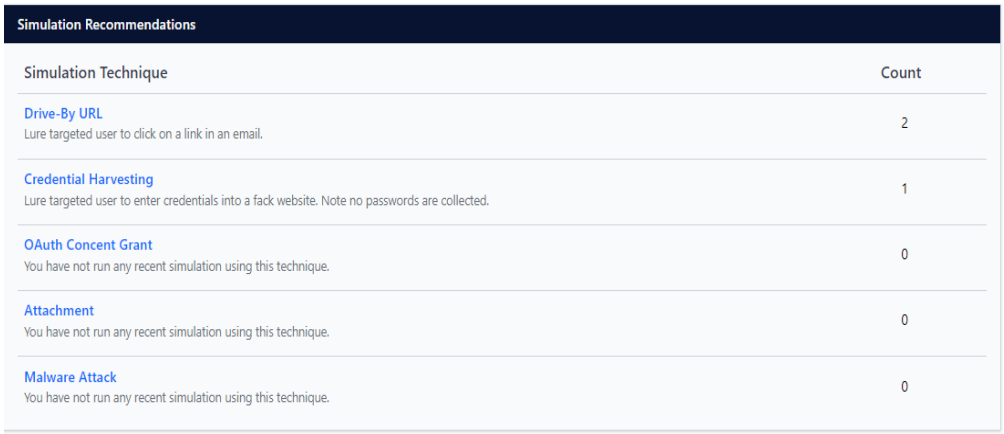

Figure 4.25. Simulation Recommendations

4.3.6 Security Awareness Training (Training Hub)

The tool provides OOTB security awareness training. This training is provided to those users who compromised in any simulation. The different training delivery methods have different outcomes on the learners' ability to recognize and mitigate phishing threats [37, 38]. This tool provides Video-based and interactive game-based security trainings to the end-users.

- **Video-Based Training**

  This tool provides video-based security training. Video-based learning is flexible, and users can watch and re watch the videos as they wish [39]. This training provides various phishing attacks awareness. They covered phishing awareness, credential harvesting, WFH, ransomware attacks, how to spot phishing and many more. Currently, the tools have training in just English language.

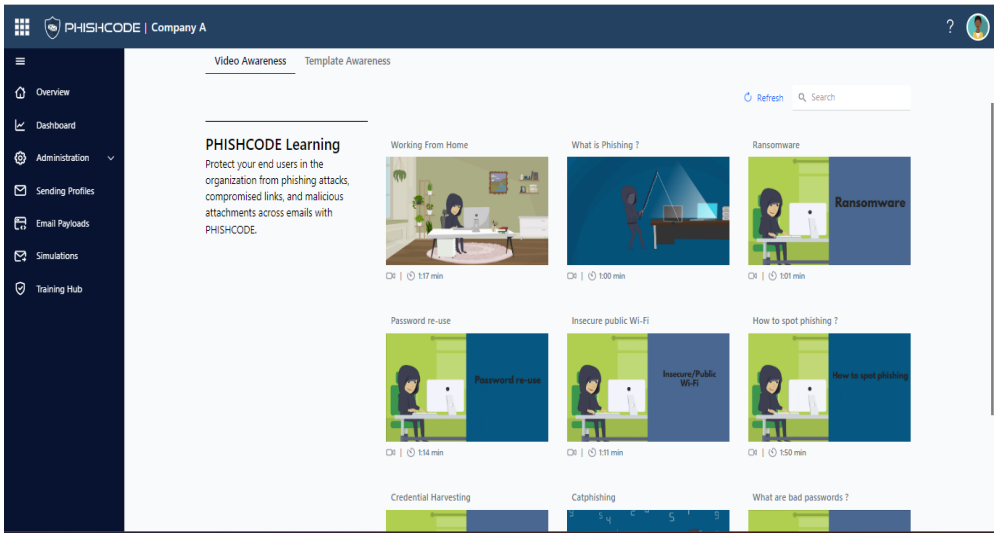

Figure 4.26: Video Awareness hub

- **Interactive Game-based Training:**

  The game-based interactive training provides end-user to learn the different components of phishing and also the points from where the user can take the right actions after learning. The game-based training provides real-time insights to the end user about their actions in the game with proper explanation. These games are designed in such a way, the end user needs to evaluate all the points to give their verdict about the legitimacy of the email [37] and these trainings also provide feedback at the same time [40].

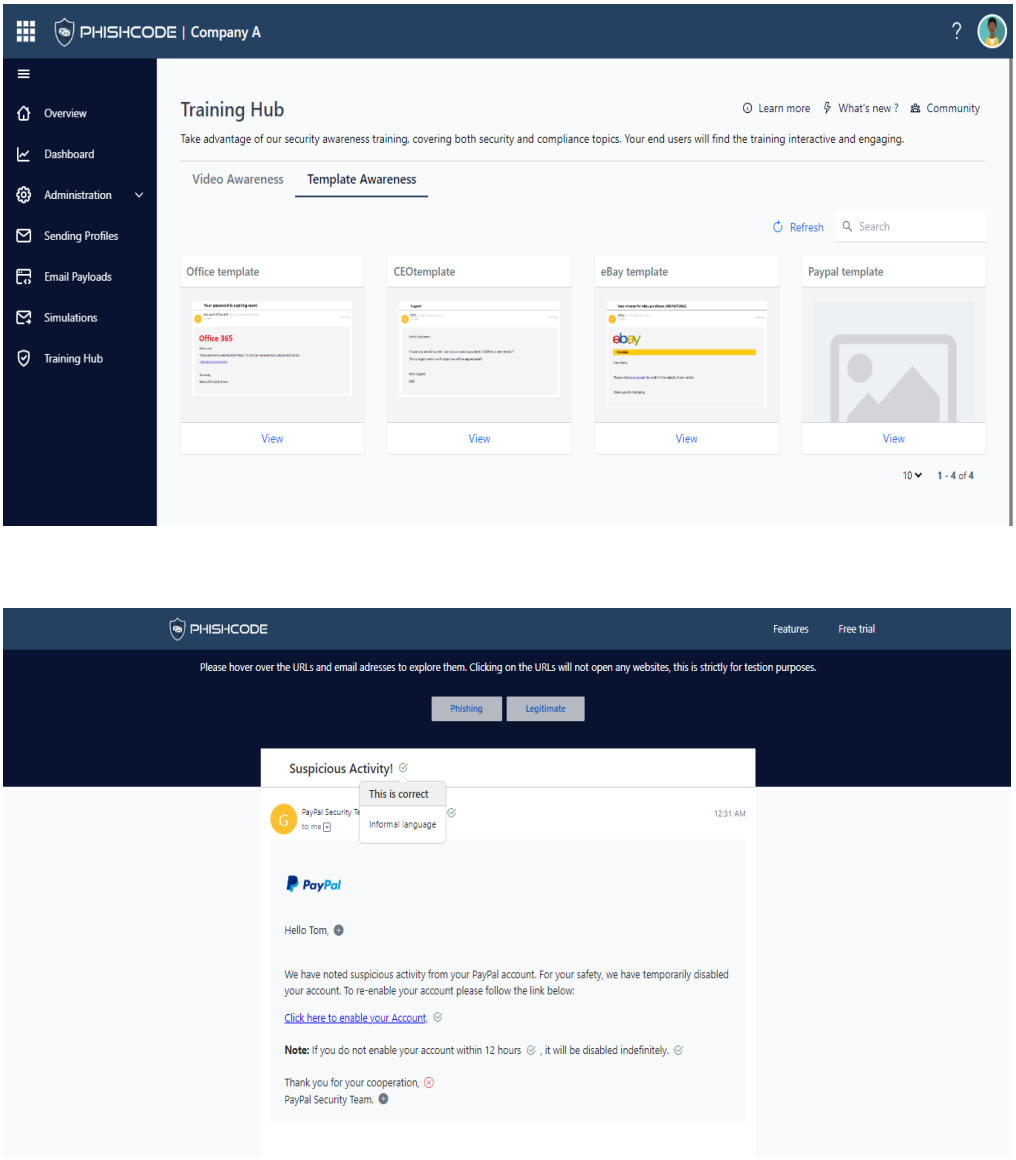

Figure 4.27: Game-based Awareness

Chapter 5

Results and Scenarios

This research conducted in two weeks' time spam to evaluate the most effective method to enhance the security awareness of the end-user which helps in reducing the phish-prone of the organization. This tool also filled all the gaps of existing phishing simulation workflow and technological gaps of tool like goPhish using by company X to evaluate their human attack surface.

We used Cyber drill to evaluate the human risk, track awareness and organizational responses against this vulnerability. Each phase contains the identical users which involved in attack simulation. In each phase, we used the different email payloads but the attack techniques is same in each phase which is credential harvesting. The summary of both phases is given below in Table 5.1.

Phase	Template	Attack Technique	Delivered	Opened	Compromised	PPP
1	account expiration	Credential harvesting	20	17	11	55%
2	Message Return	Credential harvesting	20	18	3	15%

Table 5.1. Phases Simulation Summary

5.1 Phases Evaluation

Phase 1: Results

Gathering and validating the data from Company X for the CyberDrill phase 1. In the phase one, Company X sent the "account expiration" template. In this template, we performed the targeted attacks on the 20 selected users and create the urgency for deleting your accounts within short amount of time. This payload has embedded link of the landing pages, which explains about the benign phishing attack and some information about the attack. After the completion of "account expiration" attack

simulation, we collected the data from the Company X and divided the data into 7 categories, like Email Sent, Email Opened, Not opened, Email Reported, caught or compromised user (Clicked on link), User Trained, and Repeat Offenders.

In the CyberDrill phase 1, we have following data in **chart 5.1**

- **Email Sent:** The email sent to all selected 20 users. The email sent status is 100%
- **Email Opened:** The 17 users opened the email. The email opened by 85%.
- **Unopened Email:** The 3 users did not response to the simulation. The unopened email by 15%
- **Email Reported:** No user has reported the email to the team and the status is 0%.
- **User Caught:** Those user who clicked on the benign malicious link and total 11 user performed insecure action. The user caught by 55%.
- **Repeated Offenders:** Those users who caught in multiple attack simulations campaigns. The offenders are 7 (35%).

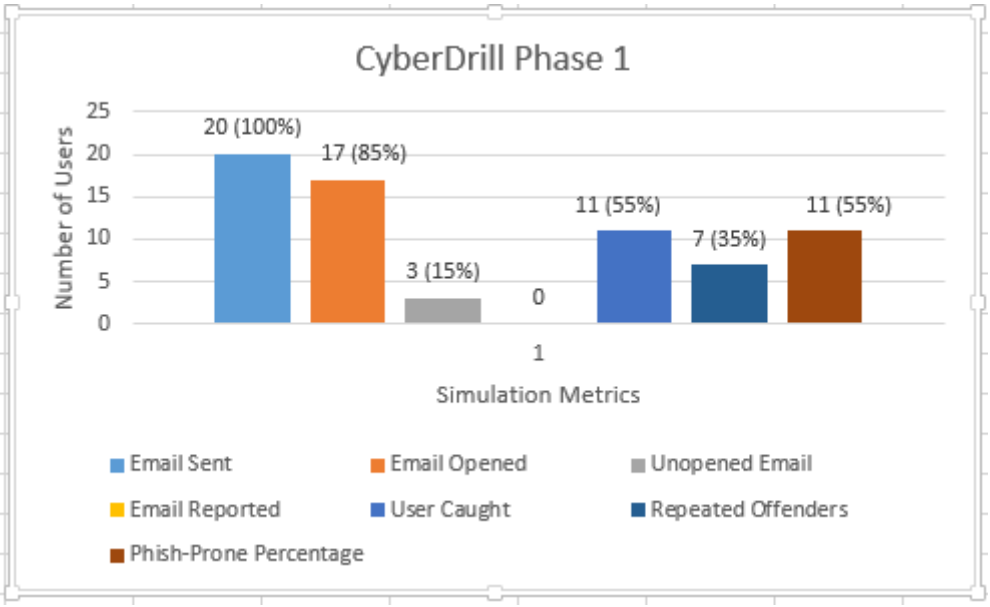

Figure 5.1: Phase 1: Attack Simulation Statics

Furthermore, the proposed tool also calculated the “Phish-prone” percentage of the organization the first phase. Figure 5.2

$$\textbf{Phish-prone Percentage} = \frac{\text{Total number of failures}}{\text{Total number emails sent.}} \times 100$$

In phase 1, total 20 emails sent to the selected users. In that simulation, 11 user compromised in this attack. So, the phish-prone percentage of organization X in phase 1 will be calculated as 11 divided by 20 which will be 0.55 and then multiply by 100. The PPP is 55%.

Figure 5.2: Phase 1: Phish-Prone Percentage (PPP)

Phase 2: Results

After 1st week, Company X again run the Attack simulation on the same selected users. Gathering and validating the data from Company X for the CyberDrill phase 2. In the phase two, Company X sent the "message returned" template. In this template, we performed the targeted attacks on the 20 selected users and create the urgency for deleting your accounts within short amount of time. This payload has embedded link of the landing pages, which explains about the benign phishing attack and some information about the attack. After the completion of "account expiration" attack simulation.

In the CyberDrill phase 1, we have following data in Figure 5.3

- **Email Sent**: The email sent to all selected 20 users. The email sent status is 100%.
- **Email Opened**: The 18 users opened the email. The email opened by 90%.
- **Unopened Email**: The 2 users did not response to the simulation. The unopened email by 10%.
- **Email Reported**: 4 users have reported the email to the team and the status is 20%.
- **User Caught**: Those users who clicked on the benign malicious link and total 3 user performed insecure action. The user caught by 15%.
- **Repeated Offenders**: Those users who caught in multiple attack simulations campaigns. The offenders are 3 (15%).

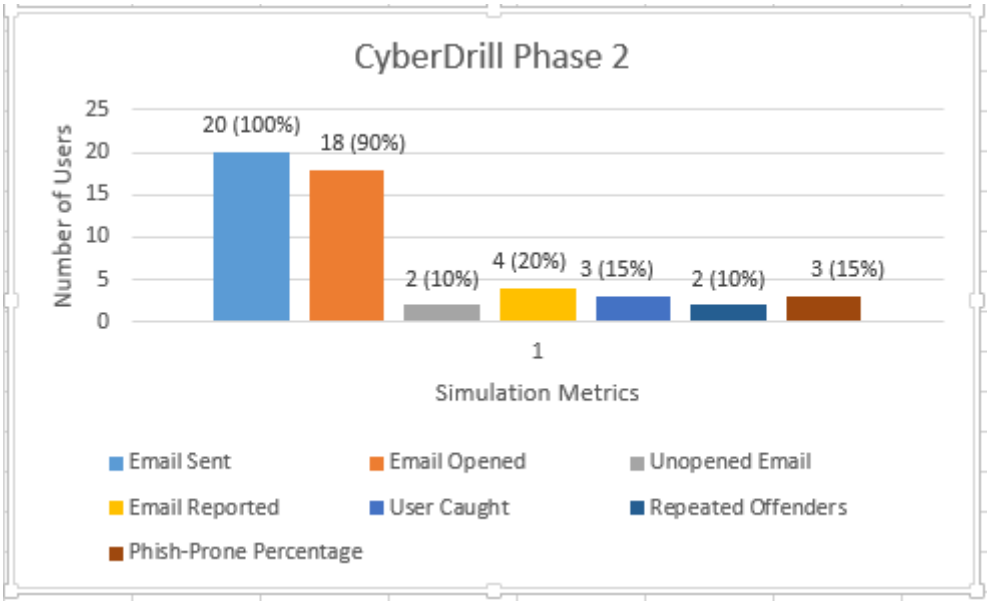

Figure 5.3: Phase 2: Attack Simulation Statics

Furthermore, the proposed tool also calculated the “Phish-prone” percentage [9] of the organization for the second phase. Figure 5.4

Figure 5.4: Phase 2: Phish-Prone Percentage (PPP)

5.2 Calculate Percentage Change rate

We are comparing the percentage decrease of phase 1 and phase two. We have seen significant improvement in Company X human risk posture. As, the email read attempt increase by 5%, email reporting increase by 20%, user awareness against the phishing attacks or caught per simulation decrease by 40%, the repeated offenders also show significant decrease by 25% through security awareness security program. The complete process also show impressive decrease in human attack surface by 40% through awareness. The PPP (Phish-Prone Percentage) or user susceptibility against attack show improvements.

Change in the percentage is calculated by following formula.

$$\textbf{Percentage Change} = \frac{(V2-V1)}{|V1|} \times 100$$

Percentage Change rate (%)

Category	Change rate (%)
Email Sent	0%
Email Opened	↑ 5.9%
Unopened Email	↓ 33.33%
Email Reported	↑ 20%
User caught	↓ 72.72
Repeated Offenders	↓ 71.42
Phish-Prone Percentage	↓ 72.72

Table 5.2. Change Rate

5.3 Summary

This chapter described the gaps identified in the phishing simulation and security awareness for company X. to address the gaps in previous program the proposed tool provides better solution and improve the human risk posture against phishing attacks. The figure 5.1, 5.2, 5.3 and 5.4 compare the processes, identified the gaps, improve the process and show the risk metrics. By gathered data it is proved that the current proposed tool has revamp the complete structure of security awareness.

Chapter 6

DISCUSSION, CONCLUSION AND FUTURE WORK

DIRECTIONS

The main purpose of this research is to enhance the human awareness against the world largest attack surface which is a phishing attack. A lot of work is done for the betterment of the phishing detections, but the most valuable and important vulnerability is still needs to be focus. The most vulnerable and easy targets are the end users who can easy exploited by simple and most sophisticated techniques and companies lost reputation, data, and money in these attacks.

In chapter 2 Literature review, we have covered the existing phishing simulation and awareness model, techniques and highlight all the challenges which currently organizations are facing within their security awareness programed to reduce the phishing risk and enhance the human awareness. In chapter 3, we have discussed the current model and the principles through which have built our proposed tool.

In the proposed tool, we have filled all the existing gaps and built all in one solution for the end user awareness against the phishing attacks. This tool has feature of multi-tenancy to add many programs in a single solution. This proposed tool, provides the OOTB email payloads, landing pages, login pages, user management, sending profiles and attack simulations. The admin can run the simulation and track it's all metrics within a single dashboard. This at a glance dashboard provides the attack coverage, organizational susceptibility against attacks, phishing risk, and progress of security awareness.

For practical evaluation of the proposed tool, we worked with the Company X to evaluate it's effectiveness. Firstly, we analyzed the current phishing simulation and awareness program. We found many gaps and security concerns within their workflow.

In their previous workflow, the email payloads were not up to the mark, no proper security weakness evaluation and development. Also, gaps within the simulation insights like no track of security awareness program progress, phishing risk assessment, repeated offenders, and security posture of the organization.

After the discussion, we implemented the proposed solution for their organization. The solution provided the fine-grained visibility around the complete organization phishing risk and also provided the step by step guidance to organization how to launch the effective evaluation and trained the end user against the phishing attacks. This solution also not only evaluate the current state of organization also predicts the susceptibility of user against each type of phishing technique so that organization can educate the risky users.

After implementation the data was gathered from the organization. We evaluate the previous state of the users and also the current state after the simulations and awareness. We analyzed the improvements on percentage change formula and found significant drop age in their phishing risk and also found significant improvement in their human awareness. This highlight that the proposed solution is highly effective for the organization.

6.1 Conclusion

Thus, this study has proven that correct and effective template built on Cialdini and 6 principles of persuasion and cyber drill method is highly effective to reduce the organizational risk against phishing attacks. Appropriate security evaluation and program enhance the end user weakness which helps users to identify the phishing attacks, reduced the susceptibility, and increase the reporting of attacks.

6.2 Future Work

For future work, an AI-driven user evaluation can be added into the tool which can track the user actions against the benign phishing attacks and predicts the user's susceptibility behavior to phishing against each technique. By the help of this the organizations assigned them the required trainings to mitigate the vulnerability. The second direction could be to build an extension, which provides its verdict and recommendations to end user so that the user can take secure actions against the suspicious email.

References

[1] Investigation, F. B. O. Business E-mail Compromise The 12 Billion Dollar Scam. [accessed 2020 Dec 12]. https://www.ic3.gov/Media/Y2018/PSA180712.

[2] Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. J Inform Secur Appl. 2015;22:113–22. doi:10.1016/j.jisa.2014.09.005.

[3] A. Alnajim, "A country based model towards phishing detection enhancement," Int. J. Innov. Technol. Explor. Eng., vol. 5, no. 1, pp. 52–57, 2015.

[4] Jampen D, Gür G, Sutter T, Tellenbach B. Don't click: towards an effective anti-phishing training. A comparative literature review. Human-centric Comp Inform Sci. 2020;10:1–41. doi:10.1186/s13673-020- 00237-7.

[5] Zwilling M, Klien G, Lesjak D, Wiechetek Ł, Cetin F, Basim HN. Cyber security awareness, knowledge, and behavior: a comparative study. J Comput Inf Syst. 2020;1–16. doi:10.1080/08874417.2020.1712269.

[6] Sun JC-Y, Yu S-J, Lin SS, Tseng -S-S. The mediating effect of anti-phishing self-efficacy between college stu dents' internet self-efficacy and anti-phishing behavior and gender difference. Comput Human Behav. 2016;59:249–57. doi:10.1016/j.chb.2016.02.004.

[7] Gabriel, B. A., & Mohamed, A. (2011). Impact of globalization. European Business Review, 23(1), 120-132. https://doi.org/10.1108/09555341111098026

[8] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," Arab. J. Sci. Eng., vol. 45, no. 4, pp. 3171–3189, 2020, doi: 10.1007/s13369-019-04319-2.

[9] Knowbe4, "PHISHING BY 2018 Phishing By Industry Benchmarking Report," p. 12, 2018.

[10] Atkins B, Huang W. A study of social engineering in online frauds. Open J Soc Sci. 2013;1:23. doi:10.4236/ jss.2013.13004.

[11] Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. J Inform Secur Appl. 2015;22:113–22. doi:10.1016/j.jisa.2014.09.005.

[12] W. Yeoh, H. Huang, W. S. Lee, F. Al Jafari, and R. Mansson, “Simulated Phishing Attack and Embedded Training Campaign,” J. Comput. Inf. Syst., vol. 62, no. 4, pp. 802–821, 2022, doi: 10.1080/08874417.2021.1919941.

[13] CYBSAFE, “A more intelligent way to reduce the threat posed by phishing attacks”. 06-06-2020

[14] W. J. Gordon et al., “Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system,” J. Am. Med. Informatics Assoc., vol. 26, no. 6, pp. 547–552, 2019, doi: 10.1093/jamia/ocz005.

[15] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, and L. Coventry, “Phishing simulation exercise in a large hospital: A case study,” Digit. Heal., vol. 8, 2022, doi: 10.1177/20552076221081716.

[16] D. Lain, K. Kostiainen, and S. Capkun, “Phishing in Organizations: Findings from a Large-Scale and Long-Term Study,” Proc. - IEEE Symp. Secure. Priv., vol. 2022-May, pp. 842–859, 2022, doi: 10.1109/SP46214.2022.9833766.

[17] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs, “Who Falls for Phish ? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions”.

[18] F. Carroll, J. A. Adejobi, and R. Montasari, “How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society,” SN Comput. Sci., vol. 3, no. 2, pp. 1–10, 2022, doi: 10.1007/s42979-022-01069-1.

[19] N. Nachin, C. Tangmanee, and K. Piromsopa, “How to Increase Cybersecurity Awareness” ISACA J., vol.2, pp. 45-50, 2019.

[20] B. M. Riggins, “PhishProof Report: How to Decrease Phishing Email Click Rates”.

[21] P. K. Yeng, M. A. Fauzi, B. Yang, and P. Nimbe, “Investigation into Phishing Risk Behaviour among Healthcare Staff,” pp. 1–30, 2022.

[22] W. Yeoh, H. Huang, W. S. Lee, F. Al Jafari, and R. Mansson, “Simulated Phishing Attack and Embedded Training Campaign,” J. Comput. Inf. Syst., vol. 62, no. 4, pp. 802–821, 2022, doi: 10.1080/08874417.2021.1919941.

[23] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, Don’t click: towards an effective anti-phishing training. A comparative literature review, vol. 10, no. 1. Springer Berlin Heidelberg, 2020. doi: 10.1186/s13673-020-00237-7.

[24] W. J. Gordon et al., “Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system,” J. Am. Med. Informatics Assoc., vol. 26, no. 6, pp. 547–552, 2019, doi: 10.1093/jamia/ocz005.

[25] B. M. Riggins, “PhishProof Report: How to Decrease Phishing Email Click Rates”.

[26] A. A. Alhashmi, A. Darem, and J. H. Abawajy, “Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats,” Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 10, pp. 29–35, 2021, doi: 10.14569/IJACSA.2021.0121004.

[27] F. Carroll, J. A. Adejobi, and R. Montasari, “How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society,” SN Comput. Sci., vol. 3, no. 2, pp. 1–10, 2022, doi: 10.1007/s42979-022-01069-1.

[28] “Gartner Research.” [Online]. Available: https://www.gartner.com/it glossary/software-a-service-saas/.[Accessed: 24-Mar-2018].

[29] E. Buchanan, J. Aycock, S. Dexter, D. Dittrich, and E. Hvizdak, “Computer Science Security Research and Human Subjects: Emerging Considerations for Research Ethics Boards,” J. Empir. Res. Hum. Res. Ethics, vol. 6, no. 2, pp. 71–83, 2011.

[30] Sheng S, Magnien B, Kumaraguru P, Acquisti A, Cranor LF, Hong J, Nunge E. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In: Proceedings of the 3rd symposium on Usable privacy and security. Pittsburgh (PA); 2007. p. 88–99.

[31] P. Kim, J. V. Homan, and R. L. Metzer, "How long do employees remember information security training programs? A study of knowledge acquisition and retention," Issues in Information Systems, vol. 17, no. 4, pp. 197–207, 2016.

[32] N. Athanassoulis and J. Wilson, “When is deception in research ethical?,” Clin.Ethics, vol. 4, no. 1, pp. 44–49, 2009.