National College of Ireland

Enhancing Cybersecurity through Comprehensive User Training Programs: A Study on Mitigating Social Engineering Threats

MSc Industrial Internship
MSc in Cybersecurity

Olumide Oladapo Banjo
Student ID: x22181539

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Olumide Banjo
Student ID:	x22181539
Programme:	MSC CYBERSECURITY **Year:** 2023
Module:	MSc Internship
Supervisor:	Vikas Sahni
Submission Due Date:	05/01/2024
Project Title:	Enhancing Cybersecurity through Comprehensive User Training Programs: A Study on Mitigating Social Engineering Threats
Word Count:	7247
Page Count:	22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Olumide Banjo

Date: 1/2/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Cybersecurity through Comprehensive User Training Programs: A Study on Mitigating Social Engineering Threats

Olumide Oladapo
Banjo
x22181539

Abstract

In order to successfully mitigate the growing threat posed by social engineering attacks, this study sheds light on the importance of user training programs specifically focused on the behavioural changes, confidence levels, threat perception and decision-making patterns.

A mixed-methods approach was adopted, engaging 30 participants from various cybersecurity backgrounds. Utilizing purposive sampling, a wide range of experiences was captured to understand the effectiveness of cybersecurity training. Both quantitative surveys and qualitative simulated social engineering attacks were combined to assess participant's vulnerabilities and the impact of the training program, before and after its implementation.

1. Introduction

Cybersecurity has continually evolved to address the dynamic range of digital threats since its inception (Wang, Sun, and Zhu, 2020). Initially, efforts were predominantly centered on technology, aiming to secure network perimeters and fortify systems. With the realization that human elements could pose security vulnerabilities (Torten, Reaiche and Boyle, 2018), cybersecurity strategies began to incorporate approaches focusing on the human aspect (Hove, 2020).

The rise in cyber threats necessitated the development of cybersecurity awareness programs to tackle the psychological aspects of cyber threats (Syafitri et al., 2022). These initiatives stemmed from the need to address the growing susceptibility of individuals and the limitations of purely technological defences (Rains, 2020). The objective was to nurture a strong cybersecurity mindset among employees, thereby reducing incidents caused by human errors (Bernier, 2020).

The escalation in social engineering attacks (see Figure 1.1 for a timeline) presented new challenges, exploiting human psychology to circumvent technological defenses (Moustafa, Bello and Maurushat, 2021). This led to the incorporation of such threats in training programs, emphasizing the importance of alertness and awareness of deceptive methods (Salahdine and Kaabouch, 2019; Mouton et al., 2014).

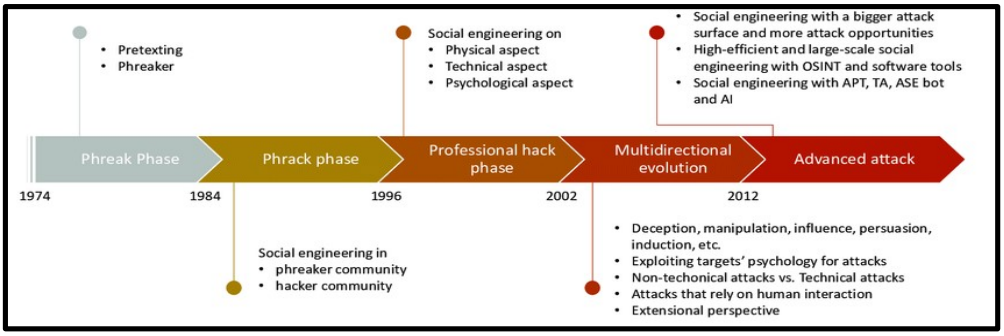

Figure 1: The Evolution of Social Engineering in Cybersecurity (Wang et al., 2020)

Presently, these educational initiatives dedicated to digital security face considerable challenges. Firms encounter significant hurdles in instilling robust digital security practices (Aldawood and Skinner, 2018; Campbell, 2019), while workforce compliance with digital security protocols frequently falls short (Torten, Reaiche and Boyle, 2018). Furthermore, the convergence of private and work-related digital environments introduces fresh security risks (Arabia-Obedoza et al., 2020).

In spite of these educational efforts, the persistence of deceptive cyber maneuvers suggests a profound deficiency. The complex dynamics of individual actions and choices further entangle the crafting of effectual educational programs (Syafitri et al., 2022), while the ever-evolving and creative strategies of cyber manipulators persistently test existing defences (Wang, Sun, and Zhu, 2020).

1.1. Statement of the Problem

This research is centered on the critical juncture where cybersecurity intersects with the rising occurrences of social engineering attacks and scrutinizes the impact of training programs aimed at raising awareness. Despite the body of research highlighting the escalating risks associated with social engineering tactics, there remains an incomplete grasp of the ways in which educational interventions can bolster an individual's defences against such attacks (Dabke, Gadgil and Dabke, 2023; Moustafa, Bello and Maurushat, 2021).

Often established as a safeguard, the disparate outcomes of these training initiatives provoke a re-examination of their conceptualization, implementation, and assessment processes. Moreover, existing research often emphasizes technical security measures, overlooking the crucial human element intrinsic to social engineering (Bernier, 2020).

Prevailing approaches to curtailing the threats from deceptive manipulation tactics often overlook the nuanced aspects of human actions (Osuagwu et al., 2015), consequently constraining their capacity to counteract the assortment of weaknesses exploited by deceptive strategists (Salahdine and Kaabouch, 2019). Additionally, the swiftly evolving cyber threat landscape underscores the insufficiency of static, uniform solutions. Consequently, this research aspires to offer a detailed understanding of the multifaceted nature of the problem at hand.

1.2. Research question

Considering the critical aspect examined in the research problems, the primary inquiry for this study would be:

- ***How can organizations design and implement customized user training programs to effectively mitigate social engineering risks, and what key***

elements are essential for enhancing cybersecurity resilience in the face of evolving social engineering threats?

1.3. Structure of the Paper

In Section 2, the existing literature concerning user training programs and strategies to counteract social engineering attacks is discussed. Section 3 elucidates the methodology employed to implement the suggested approach. Section 4 details the design specifications of the proposed approach. In Section 5, a comprehensive account of the implementation process is provided. Concluding the discussion, Sections 6 and 7 cover the assessment results and draw conclusions based on the findings.

2. Related work

2.1 Literature Review

2.1.1 Development of Digital Security

The rise of digital security parallels the emergence of the digital era, evolving in tandem with advancements in information technology. Initially, its primary objective was to protect systems from external intrusions and reduce the risks of data breaches. Methods like firewalls and antivirus solutions were created to combat these external threats (Campbell, 2019). As technology advances, cyber threats, including sophisticated forms like social engineering, have proliferated. Social engineering exploits individual vulnerabilities rather than system weaknesses, with the variable nature of human behavior identified as a key factor in its effectiveness, despite robust technological safeguards (Fan & Rong, 2017; Ivaturi & Janczewski, 2011)

Digital security measures have evolved to include human factors, emphasizing a comprehensive approach (Klimburg-Witjes and Wentland, 2021). This perspective recognizes personnel as central to the cybersecurity framework, acknowledging their role as both defenders and potential vulnerabilities. Consequently, current measures aim to incorporate frameworks reflecting the impact of human actions on security protocols. Investigations emphasize the critical role of user training in addressing cyber threats, especially those related to social engineering (Bada et al. 2019). However, challenges arise due to the complexities of human nature, hindering the efficacy of education programs. This underscores the shift from technical solutions to a holistic, human-centric approach in enhancing staff awareness of cybersecurity measures.

2.1.2 Digital Security Training Programs

Profoundly implemented programs for cyber safety consciousness are essential for mitigating the risks of manipulative cyber tactics. These educational series recognize the criticality of human participation in upholding digital security. Their objectives include expanding insights into digital dangers, enforcing adherence to data protection regulations, and emphasizing the human vulnerabilities targeted by manipulative cyber techniques (Mouton et al. 2014).

These initiatives vary in substance, concentrating on elevating alertness to digital menaces (Albladi and Weir 2018), improving organizational cyber literacy, and imparting actionable security methods. They further endeavor to transform perceptions and conduct concerning cyber safety, given that user perspectives substantially influence their protective behaviours.

2.1.3 Manipulative Cyber Strategies

The incidence of manipulative cyber strategies is on the rise, complicating the landscape of cyber dangers (Ghafir et al., 2016; Wang, Sun and Zhu, 2020). These strategies, which range from phishing to pretexting, exploit human traits rather than software flaws (Fan, Kevin and Rong, 2017). The effective manipulation of human characteristics is a concern, as factors like impulsivity and personality traits can make individuals more vulnerable to such attacks (Hove, 2020; Klimburg-Witjes and Wentland, 2021).

Countermeasures such as cybersecurity awareness training have been advocated to combat these threats (Rains, 2020; Salahdine and Kaabouch, 2019). Nevertheless, the challenge persists in translating increased awareness into behavioural change (Siddiqi and Siddiqi, 2022). Current research and practice must focus on strengthening human defences and awareness, alongside continual evaluation and adaptation of methods to address the evolving nature of these threats.

2.1.4 Dynamics Between Cyber Safety Education and Manipulative Cyber Strategies

Investigations Education focused on cyber safety awareness has been shown to significantly reduce manipulative cyber activities. Comprehensive knowledge enables individuals to detect and avoid fraudulent tactics, reducing related dangers (Aldawood and Skinner, 2018). In organizations, security knowledge is crucial for a strong defense against cyber-attacks, with heightened vigilance inversely related to vulnerability (Campbell, 2019). However, there is a challenge in translating cyber safety awareness into behavioral change, highlighting a disconnection between knowledge acquisition and real-world actions (Syafitri et al., 2022). Individual factors such as temperament, cognitive inclinations, and decision-making processes play a significant role in responses to threats (Wilcox and Bhattacharya, 2016).

The Protection Motivation Theory (PMT), incorporating perceptions of vulnerability, threat severity, response effectiveness, and self-efficacy, is being used in cyber safety programs with positive outcomes (Spinapolice, 2011; Torten et al., 2018). However, the link between cyber security training and behavioral responses to social engineering threats is complex, with knowledge of policies not always ensuring compliance (Saleem and Hammoudeh, 2018). Additional factors, such as perceived risk, may influence the impact of policy awareness on cybersecurity practices (Arabia-Obedoza et al., 2020).

While awareness is essential, it alone is not enough to ensure secure practices; the perceived gravity of threats also influences user behavior. Training should aim to alter attitudes and behaviors, not just disseminate knowledge, as good intentions do not always lead to secure actions (Alharthi and Regan, 2020).

2.1.5 Deficiencies in Existing Studies

Despite significant efforts in digital security research, notable deficiencies persist, providing opportunities for future refinement (Aldawood and Skinner, 2018). A key shortfall lies in the limited exploration of how instructional programs impact the reduction of risks associated with deceptive cyber strategies in diverse business settings. While personal attributes influencing digital security conduct have been studied, a scarcity of insights into their collective influence on susceptibility to deceptive cyber activities remains. An integrated analysis of these traits could enhance customized and effective digital security education.

The role of corporate ethos in susceptibility to deceptive cyber activities requires

further examination, given the exploitation of behavioral and cognitive predispositions. Understanding cultural aspects within organizations is crucial for addressing this issue (Fan, Kevin, and Rong, 2017). Disagreement persists on optimal methods for assessing the outcomes of digital security awareness education as cyber risks evolve. This study aims to fill these gaps by focusing on the effectiveness of digital security training against deceptive cyber strategies, considering individual characteristics, organizational culture, evaluation methodologies, and demographic factors for a comprehensive understanding. Additionally, extending research beyond the user perspective to incorporate insights from IT experts and policy framers is crucial (Rains, 2020; Wang et al., 2020).

2.2 Conceptual Framework

2.2.1 Theory of Digital Information Security

The Theory of Digital Information Security (DIS) provides a critical analytical angle for enhancing protective behaviours, particularly in countering deceptive digital tactics (Arabia-Obedoza et al., 2020). This theory focuses on defending data against unsanctioned access and underpins the foundation of this study: the essentiality of all-encompassing digital safety education (Syafitri et al., 2022). DIS posits that, apart from technical barriers, recognizing human behaviour's is key in reducing the effectiveness of deceptive digital strategies (Torten, Reaiche and Boyle, 2018). Research such as that by Salahdine and Kaabouch (2019) validates DIS's utility, indicating that heightened awareness of policies enhances adherence to security protocols. Nevertheless, DIS's application is typically constrained to internal organizational contexts, emphasizing influences on internal conduct (Wilcox and Bhattacharya, 2016). Broadening its scope to encompass societal vulnerabilities to such threats requires thoughtful adaptation to maintain relevance in varied contexts. Therefore, tactful utilization of DIS in this study provides an extensive viewpoint for evaluating the influence of user education in countering the risks posed by social engineering.

2.2.2 Theory of Behavioural Social Dynamics

The Theory of Behavioural Social Dynamics (BSD) provides a robust psychological framework for understanding human behaviour within social contexts, emphasizing the interconnectedness of individual, environmental, and behavioural factors (Aldawood and Skinner, 2018). BSD's relevance in cybersecurity, particularly in assessing the effectiveness of awareness training against deceptive tactics, is increasingly recognized (Rains, 2020). It acknowledges the significance of environmental and social influences, in shaping cybersecurity behaviour. BSD is especially relevant to social engineering tactics, which often depend on manipulating social perceptions (Campbell, 2019). It underscores the importance of learning through observation and self-efficacy in response to cybersecurity training (Dabke, Gadgil and Dabke, 2023). However, BSD might not cover all aspects, possibly overlooking systemic factors like organizational policies (Ghafir et al., 2016). Thus, integrating BSD within a broader organizational context can offer a comprehensive understanding of the dynamics at play in cybersecurity awareness and training effectiveness.

2.2.3 Protection Motivation Theory

The Protection Motivation Theory (PMT) is crucial for understanding individuals' responses to cybersecurity threats, emphasizing cognitive assessments of

danger and coping abilities. PMT links to adaptive protective behaviors in cybersecurity but faces criticism for its limited impact on behavioral change and challenges in addressing varied cognitive processes. It may not fully capture nuances in behaviors like social engineering, necessitating a nuanced approach. Combining PMT with Information Security Theory and Social Cognitive Theory creates a robust framework for understanding the effectiveness of cybersecurity training programs, considering human elements, cognitive processes, and motivational factors. This synthesis provides a comprehensive perspective for addressing research questions in the field.

3. Research Methodology

This study focused on examining the effectiveness of cybersecurity training in thwarting social engineering. It entails a thorough literature review, collection of empirical data through surveys and controlled attack simulations, and the formulation of informed guidelines to refine the training initiatives.

3.1 Research Design

Employing a mixed-methods strategy, quantitative and qualitative data was integrated to explore human behaviour and response to social engineering and cybersecurity training. This approach has been validated in prior studies for its capacity to capture the multifaceted nature of cybersecurity. The dual lenses of this method enhance the depth and credibility of the findings.

The chosen mixed-methods framework combines the depth of qualitative insights with the clarity of quantitative analysis, revealing the intricate interplay of human, organizational, and technological factors in cybersecurity (Creswell and Creswell, 2017; Almalki, 2016). Alternative singular methodologies were discarded as they do not sufficiently reflect the complexity of cybersecurity's challenges.

The guiding questions demand an exploration of both the existing literature and practical engagement with cybersecurity training. The study's structure, inspired by previous research, incorporates a mixed-methods design with surveys, simulations, and literature review. This blend affords a multi-faceted perspective, aligning theoretical knowledge with empirical findings, thus providing a holistic view of the cybersecurity training landscape and revealing avenues for its enhancement.

3.2 Collection of Data

3.2.1 Surveys

Surveys were structured to gauge the attitudes of employees and their reactions towards social engineering threats and their views on cybersecurity training, following the framework suggested by Arachchilage and Love (2014). Conducted online for efficiency, steps were taken to encourage participation and account for potential non-response.

3.2.2 Simulated Social Engineering Attacks

To evaluate vulnerability to social engineering, simulations were created. Participants were thoroughly debriefed afterwards to clarify the exercise and address any concerns, maintaining ethical standards. Participant interactions were meticulously documented to enrich the analysis, as suggested by Mouton *et al*. (2016).

3.3 Data Analysis

The data analysis undertaken in this study is two-fold, addressing both

quantitative and qualitative aspects. Together, they form a comprehensive appraisal of the efficacy of cybersecurity training initiatives.

3.3.1 Quantitative Data Analysis

Statistical evaluations of survey responses constitute the quantitative analysis. Using descriptive statistics such as mean, median, mode, and standard deviation, this phase examines connections between variables and discerns recurring trends in the dataset. The aim is to interpret these statistics to gain insights into employee perceptions and behaviours concerning social engineering and the corresponding cybersecurity training. It is acknowledged that quantitative data may not capture the full subtlety of respondent attitudes (Arachchilage & Love, 2014).

3.3.2 Qualitative Data Analysis

The qualitative analysis supplements the study by examining behaviours during simulated attacks and insights from reviewed literature. It employs thematic analysis to identify prevailing themes and concepts. This method adds depth and complexity to the understanding of cybersecurity, addressing the quantitative data's limitations.

3.4 Triangulation of Data from Different Sources

Triangulation involves corroborating findings through various data sources and methods to reinforce the study's credibility (Almalki, 2016). This study juxtaposes survey results, simulations, and literature to ensure robust and dependable conclusions, pinpointing and addressing any discrepancies.

3.5 Reliability and Validity

The study's reliability, or the consistency of its findings, is bolstered by clearly defined constructs, validated survey tools, and meticulous documentation of data procedures. Validity was assured through methods like member checking, data triangulation, and precise result interpretation. Yet, limitations and potential biases, such as sample characteristics, methodological choices, and various biases in data interpretation and literature selection, must be acknowledged and addressed for accurate result interpretation and to inform future research.

4. Design Specification

4.1 Survey Design and Implementation

Surveys designed to measure the efficacy of cybersecurity training were implemented following Arachchilage and Love's (2014) guidelines. The surveys consisted of demographic questions about age, gender, occupation, experience, and prior training, as well as queries regarding knowledge of phishing and baiting—key social engineering tactics (Koyun and Al Janabi, 2017). This method was selected to understand how different backgrounds influence training effectiveness. Online distribution ensured a broad reach and accommodated participant schedules. The response analysis utilized evaluation metrics for cybersecurity training (Koutsouris *et al*., 2021), considering participant suggestions for improvements and overall thoughts on the training received. These surveys underpinned the research's mixed-methods approach, providing quantitative data for subsequent triangulation with simulation outcomes and literature review insights.

4.2 Simulated Social Engineering Attacks

The research employed simulated social engineering attacks to evaluate the effectiveness of cybersecurity training. Participants were exposed to phishing, baiting, and pretexting attacks, mirroring real-world tactics (Koyun and Al Janabi, 2017; Krombholz *et al*., 2015). Initially, these simulations assessed their baseline susceptibility to such tactics. Post-training, identical simulations tested the training's impact on their defensive skills.

The process included sending deceptive emails (phishing), offering digital incentives (baiting), and impersonating authority figures to extract information (pretexting). These methods aimed to replicate authentic social engineering threats, enhancing the study's practical relevance. The pre-training simulations gauged the participants' initial vulnerability, providing a benchmark for post-training evaluation.

Ethical standards were strictly adhered to, with participants debriefed post-simulation to clarify the exercise's purpose and address any concerns. This approach ensured the simulations were realistic yet conducted within ethical boundaries. The detailed documentation of participant interactions enriched the analysis, providing insights into their decision-making processes and overall cybersecurity awareness (Mouton *et al*., 2016). These simulations played a crucial role in assessing the practical applicability of the cybersecurity training and its efficacy in real-world scenarios.

4.3 Training Program Design

The cybersecurity awareness training program, informed by current best practices (Kim and Beuran, 2018), was meticulously designed to equip participants with skills to recognize and resist social engineering tactics. The curriculum covered a wide range of topics, from basic cybersecurity principles to advanced social engineering countermeasures (Mouheb *et al*., 2019). Instructional methods included interactive workshops, online courses, and seminars, catering to diverse learning styles (Beyer and Brummel, 2015).

4.4 Participant Selection

Participants were selected based on specific criteria (Table 2). This approach ensured a broad spectrum of experiences, encompassing both seasoned professionals and novices in cybersecurity (Chong, 2018). Such diversity was crucial for assessing the training's effectiveness across various knowledge levels.

Table 2: Eligibility Criteria for Participants

Criteria	**Description**
Criteria for Inclusion	
1. Status of Employment	Participants must presently hold a position involving engagement with IT systems
2. Training Experience	May have or have not participated in any cybersecurity awareness training programs in the last 12 months

3. Level of Experience	Participants must possess at least six months of experience in their current role to ensure familiarity with the organization's practices, or they will receive training if selected.
Criteria for Exclusion	
1. Status of Employment	Individuals who are not presently employed or in positions that do not involve interaction with IT systems
2. Level of Experience	Individuals with less than six months of experience in their current role may not be fully acquainted with the organization's cybersecurity practices

4.4.1. Ethical Consideration in Participant Selection

In cybersecurity, safeguarding the privacy and security of individuals' information is critical. Prior to their participation, individuals were fully informed about the nature of the research, their role in it, and their right to discontinue participation at any time, consistent with informed consent guidelines proposed by Creswell and Creswell (2017).

4.5 Design Relevance and Participant Preparedness

The training design's relevance was evident in its ability to enhance participants' skills in recognizing and combating social engineering threats. The program's adaptability to different experience levels ensured all participants were adequately prepared, regardless of their prior exposure to cybersecurity training.

4.6 Recommendations for Training Program Enhancement

Based on the findings, several improvements were suggested. These included incorporating more real-world examples and interactive elements to enhance engagement and retention (Koutsouris *et al*., 2021). Future chapters will detail these recommendations, focusing on practical applications.

5. Implementation

The research comprised three phases: first, a survey was deployed to assess cybersecurity awareness and training frequency across different demographics. Next, a simulated social engineering attack was conducted. Finally, a tailored training program was implemented to address the organization's needs and vulnerabilities.

5.1 Survey Deployment

Initially, a thorough survey across diverse organizational roles was conducted to assess cybersecurity awareness and training frequency among different demographics. This step was crucial to establish a baseline understanding of participants' current knowledge and identify areas requiring focused attention.

5.2 Simulated Social Engineering Attacks

To assess staff vulnerability to cyber threats objectively, controlled simulations mimicking various attack types (like phishing and pretexting) were carried out. These simulations, mirroring real-world threats, were conducted both before and after the cybersecurity training to gauge changes in participants' responses.

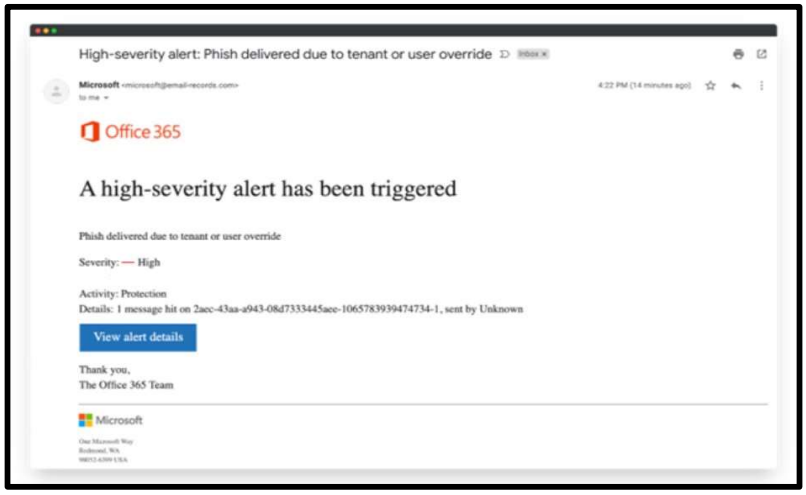

Figure 2: A fake phishing alert email screenshot from Microsoft Office 365 service

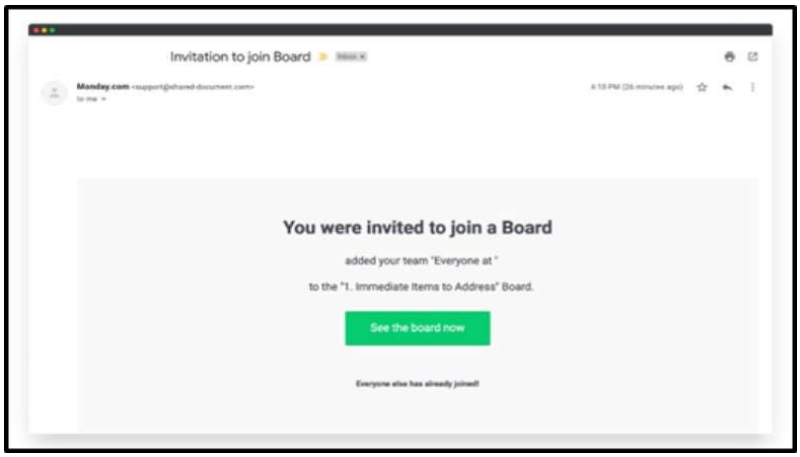

Figure 3: A fake Monday.com board invitation email screenshot with a call-to-action button.

5.3 Cybersecurity Training Program

During the implementation phase, a key focus was on creating a tailored cybersecurity training program for the organization. The training sessions were conducted in person to ensure interactivity and immediate feedback. Employees from various departments and experience levels participated, ensuring representation across the organization.

To enhance learning, the training employed diverse teaching styles, including interactive workshops, hands-on exercises, and real-world scenario analyses. Emphasizing a hands-on approach, participants engaged in practical activities simulating real cybersecurity threats in a controlled environment.

The training was designed to be dynamic, adapting to the evolving nature of cyber threats. It also addressed the importance of behavioural change, incorporating modules on fostering a security-minded culture and understanding the psychological aspects of social engineering.

The next chapter will comprehensively analyze the training program, assessing its impact on participants' attitudes and behaviors towards cybersecurity, and its overall effectiveness in bolstering the organization's resilience against social engineering threats.

6. Evaluation

This research analyzed the results from the simulated social engineering attack and the surveys designed to measure the efficacy of cybersecurity training. The discoveries were evaluated in the context of the research inquiries and goals. The presentation includes only statistical outcomes, with no disclosure of personal details like names, email addresses, or company information to uphold the confidentiality of the data.

6.1 Data Analysis Framework

This study employed a mix of surveys and simulations to evaluate how aware employees are of cybersecurity. Surveys uncovered people's views and vulnerabilities to tricks like social engineering, showing their behavior. Simulated attacks and interviews give more insights into how training works in practice and how it is perceived. This dual approach minimizes biases and enhances our understanding of training effectiveness.

6.2 Quantitative Analysis

The quantitative aspect involved a survey disseminated across diverse professional roles, alongside data from simulated social engineering attacks. The survey aimed to measure the shift in employees' awareness post-training, while the simulations tracked their interactive responses to various cyber threats before and after the training intervention.

6.2.1 Surveys

The survey sampled a broad array of professionals aged under twenty to over fifty, across diverse roles.

Age Group	Male	Female	Total
Below 20	2	1	3
20-29	5	3	8
30-39	2	4	6
40-49	4	3	7
50 and above	4	2	6

Figure 4: Information on Demographics

Figure 4 illustrates the age and gender distribution of participants. The data revealed a notable concentration among those aged 20-29 and 40-49, with eight and seven individuals, respectively.

Knowledge of Phishing	Number of Respondents
Yes	12
No	11
Uncertain	4
No Data (No training received)	3
Knowledge of Baiting	
Yes	6
No	16
Pretexting	2
No Data (No training received)	6

Figure 5: Understanding of Social Engineering Tactics

Figure 5 assessed participants' familiarity with social engineering, including phishing and baiting. Findings showed mixed levels of knowledge, with moderate to high awareness of phishing but lower awareness of subtler techniques like baiting, highlighting a knowledge gap in recognizing less obvious threats.

Training Type	Training Frequency	Number of Respondents
Workshop	Annually	3
Workshop	Bi-annually	0
Workshop	More than twice a year	5
Online Course	Annually	6
Online Course	Bi-annually	0
Online Course	More than twice a year	2
Seminar	Annually	0
Seminar	Bi-annually	5
Seminar	More than twice a year	1
No Training	Never	3

Figure 6: Training types and frequency

Figure 6 shows participants primarily engage in cybersecurity training through online courses, with a focus on annual sessions. Workshops, held more than twice a year, are also popular, while seminars are less frequent. Notably, some respondents have not undergone any cybersecurity training, indicating disparities in training participation.

Years of Experience	Number of Respondents with Training	Number of Respondents without Training
Less than 1 year	5	1
1-4 years	4	0
5-9 years	5	0
10 years or more	11	2

Figure 7: Experience and training

Figure 7 correlates professional experience with cybersecurity training. New entrants in the field were less likely to have received training while experienced professionals are more likely to have undergone it.

Suggestions for Improvement	Number of Mentions
More real-world examples/case studies	4
More frequent refreshers/assessments	4
More interactive/engaging methods	7
Update content regularly	3
More comprehensive/variety of attack types	3
No suggestion	1
Start/Implement basic training	2
Greater personal responsibility	1
Role-play simulations	1

Figure 8: Training enhancement suggestions

Figure 8 compiles recommendations for improving the training programs. The most frequent suggestion was for more engaging and interactive methods. Other notable recommendations included the use of real-world examples, regular refreshers, and comprehensive content covering a variety of attack types. This feedback emphasizes the need for dynamic, relevant, and continual training approaches.

6.2.2 Simulated Social Engineering Scenarios

The study simulated social engineering scenarios to assess the vulnerability of six participants before and after cybersecurity training. The goal was to measure the impact of training on participants' susceptibility to such attacks. The process was structured as follows:

1. ***Selection of Participants***: Six individuals were randomly selected, representing a mix of job functions and experience levels. The participants' confidentiality and anonymity were strictly maintained.
2. ***Pre-Training Simulation***: Before any training, these individuals were exposed to simulated attacks, which included sending deceptive emails. This was to gauge their initial reactions and susceptibility to these tactics.

3. ***Training Intervention:*** The participants engaged in a cybersecurity training program, designed to directly address the simulated social engineering threats they encountered.

Participant Engagement:

- **Interactive Sessions:** Participants actively participated in collaborative workshops, discussing experiences and sharing insights to foster a positive learning environment.
- **Feedback Sessions:** Post-activity feedback sessions were held, allowing participants to reflect on their performance in simulations and receive constructive criticism.
- **Questions and Clarifications:** Participants actively asked practical application questions during training and this was clarified with examples for better understanding.

4. ***Post-Training Simulation:*** Subsequent to the educational session, a replicated set of mock incursions, mirroring the initial ones, was executed to gauge the variation in the participants' reactions.

Participant	Phishing	Pretexting	Baiting	Reaction time
Participant 1	Clicked link in email	Shared sensitive information	Accepted incentive	2 hours
Participant 2	Ignored email	Did not share information	Rejected incentive	4 hours
Participant 3	Reported email	Shared partial information	Accepted incentive	1 hour
Participant 4	Clicked link in email	Did not share information	Rejected incentive	2.5 hours
Participant 5	Ignored email	Shared sensitive information	Accepted incentive	3 hours
Participant 6	Reported email	Did not share information	Rejected incentive	4.5 hours

Figure 9: Initial response to simulated attacks

Figure 9 summarizes the responses of six participants to simulated cyber-attacks. In phishing scenarios, only two individuals proactively identified and reported the attempts, while others either engaged or overlooked them, indicating potential gaps in understanding or training. In pretexting scenarios, half refrained from sharing information. Baiting responses varied, with only three people rejecting the lures. Response times ranged from 1-4.5 hours, highlighting diverse levels of alertness to cyber threats.

Participant	Phishing	Pretexting	Baiting	Reaction time
Participant 1	Reported email	Did not share information	Rejected incentive	1 hour
Participant 2	Reported email	Did not share information	Rejected incentive	2 hours
Participant 3	Ignored email	Did not share information	Rejected incentive	1.5 hours
Participant 4	Reported email	Did not share information	Rejected incentive	1 hour
Participant 5	Ignored email	Did not share information	Rejected incentive	2 hours
Participant 6	Ignored email	Did not share information	Rejected incentive	1.5 hours

Figure 10: Post-Training simulated attack outcomes

Figure 10 shows enhanced participant behaviour following training. In phishing scenarios, there was an increase in correct identification and reporting. For pretexting, all participants withheld information, a marked improvement. In baiting scenarios, all resisted the incentive, showcasing increased awareness. The response time notably decreased, suggesting heightened vigilance post-training.

Participant	Phishing	Pretexting	Baiting	Reaction time
Participant 1	Improved (Reported email)	Improved (Did not share information)	Improved (Rejected incentive)	Reduced by 1 hour
Participant 2	Improved (Reported email	No change	No change	Reduced by 2 hours
Participant 3	Regressed (Ignored email)	Improved (Did not share information)	Improved (Rejected incentive)	Reduced by 0.5 hours
Participant 4	Improved (Reported email	No change	No change	Reduced by 1.5 hours
Participant 5	No change	Improved (Did not share information)	Improved (Rejected incentive)	Reduced by 1 hour
Participant 6	No change	No change	No change	Reduced by 3 hours

Figure 11: Behavioural changes

The data in figure 11 demonstrates the positive influence of cybersecurity training, with most participants improving their response to phishing, pretexting, and baiting. However, inconsistencies were noted, including one regression case post-training. A notable uniform improvement was seen in reduced reaction times, indicating enhanced alertness.

6.3 Qualitative Assessment

Thematic analysis was utilized to explore employee behaviors and training impact during simulations. The six-phase process involved data familiarization, initial coding, theme identification, review, definition, and report compilation (Creswell and Creswell, 2017). The analysis revealed significant themes, providing insights into participant behaviors and training effectiveness. Qualitative data from interviews before and after simulations are presented in Figure 12.

Participant	**Pre-training confidence levels**	**Post-training confidence levels**	**Pre-training perceived threat level**	**Post-training perceived threat level**	**Pre-training decision making**	**Post-training decision making**
Participant 1	Low: I don't feel I know enough to protect myself.	High: I feel confident in identifying and responding to threats now.	High: I feel every suspicious mail is a potential threat.	Medium: I can now differentiate between genuine and malicious emails.	Hasty: I clicked on the link without thinking much about it.	Thoughtful: I reviewed the email carefully before reporting it.
Participant 2	Medium: I have a basic understanding of threats but not sure how to respond.	High: The training has helped me understand the best actions to take.	Low: I did not think I would be targeted.	High: I understand that anyone can be targeted and also how to spot these attempts.	Indecisive: I was not too sure so I just ignored the email.	Resolute: I identified the phishing indicators and decided to report it.
Participant 3	High: I think I am pretty aware of cybersecurity risks.	Very high: The training has reinforced my knowledge and I feel more confident now.	High: I always worry about cyber threats.	High: I still feel the threat but now I know how to respond.	Risky: I shared partial information as I thought it wouldn't cause harm.	Cautious: I did not share any information as it could be risky.
Participant 4	Low: I have heard of phishing but did not know much about it.	Medium: I have learned a lot but I feel there is more to know.	Medium: I know threats exist but I do not think about them often.	High: The training made me realize how prevalent these threats are.	Reactive: I clicked the link hoping just to know more about the email.	Analytical: I compared the email to the examples.
Participant 5	Medium: I think I can handle some threats but certainly not all.	High: I feel prepared and know what steps to take during an attack.	Medium: I am aware of threats but I didn't think they were so sophisticated.	High: The training opened my eyes to the complexity of these attacks.	Fear-driven: I felt threatened and thought sharing info may solve it.	Informed: I knew not to share sensitive information, regardless of context.
Participant 6	High: I have some experience in this area so I think I can handle it.	Very High: The training provided deeper insights, making me more confident.	Medium: I know there is risk involved, but I felt prepared for it.	Medium: The risk is the same, but my ability to handle it has improved.	Prudent: I felt the email was suspicious so I reported it.	Vigilant: I noticed the signs immediately and reported immediately.

Figure 12: Confidence levels, Threat perception and Decision-making patterns

6.3.1 Initial Data Engagement and Coding

The initial phase involved meticulously examining the data from the simulated attacks (referenced in Figure 12). This process included thorough reading and initial notation of participants' verbatim responses. Each data point was scrutinized for significant elements that could potentially emerge as repetitive patterns or themes.

6.3.2 Theme Identification and Refinement

During the theme identification stage, relevant coded data were collated to form potential themes. These were then reviewed against the dataset to ensure coherence. Any inconsistencies identified led to the refinement, combination, or exclusion of initial themes, creating a cohesive thematic structure. Subsequently, each theme was elaborated upon, defining its specific characteristics and relevance to the data.

6.3.3 Thematic Report Compilation

Concluding the study, an in-depth thematic examination was conducted, directly associating each theme with the posed inquiry. This exhaustive account detailed the shifts in the participants' perspectives and actions prior to and subsequent to the educational sessions, accentuating the efficacy of the program. Primary themes encompassed Assurance Levels, Emotional Reactions, Scale of Perceived Threat, and Analytical Decision Processes.

The programs noticeably boosted participants' confidence, particularly those who initially had lower levels. Notably, participants one and four showed significant improvement, supporting Beyer and Brummel's (2015) idea that enhanced confidence indicates effective cybersecurity training. This aligns with Beuran et al.'s (2016) finding that such training effectively addresses knowledge gaps.

After training, participants showed a shift to more positive emotions, like increased calmness. This shift is vital, as emotions directly affect cybersecurity behavior (Torten, Reaiche, and Boyle, 2018). For instance, Participant one moved from panic to calmness after training, highlighting how positive emotions influence decision-making in the face of threats.

Post training, participants significantly increased their perception of threats, highlighting the program's effectiveness in raising risk awareness. For example, Participant two's threat perception shifted from low to high, underscoring the importance of threat awareness for reinforcing secure behavior. The cybersecurity training positively influenced decision-making, enhancing participants' confidence, emotional readiness, threat awareness, and decision-making skills.

6.4 Influential Factors on Cybersecurity Training Effectiveness

The analysis delineated various factors influencing cybersecurity training effectiveness. These encompass personal attributes, organizational culture, assessment methods, demographic elements, and training program specifics.

1. ***Personal Attributes:*** Research highlights the influence of individual traits on cybersecurity behaviour (Albladi and Weir, 2018). Training can positively impact confidence, emotional responses, and decision-making, emphasizing the importance of incorporating psychological aspects into training implementation.
2. ***Organizational Culture:*** The mentioned literature indicates that organizational culture influences susceptibility to social engineering. While not explicitly examined, it is plausible that a culture promoting security and learning can improve training effectiveness.

3. ***Assessment Methods:*** Post-engagement evaluations, illustrated in Figure 10 and 11, indicate behaviour changes after training. Improved responses post-training emphasizes the value of these assessments stressing evaluation of cybersecurity conduct for training effectiveness.
4. ***Training Program Characteristics:*** The effectiveness of training is highlighted by its design, frequency, and proposed advancements. Engaging teaching strategies, practical case studies, and consistent reviews enhance its impact.

The empirical data supports existing literature on cybersecurity awareness training, emphasizing the significance of personal traits, organizational culture, measurement tools, demographics, and training characteristics. The findings highlight the importance of further research into demographics and organizational culture to enhance the effectiveness of cybersecurity training and mitigate social engineering attack risks.

6.5 Development of Artifacts

As a result of the analysis and discoveries, a comprehensive set of guidelines has been developed for cybersecurity awareness programs with the goal of mitigating social engineering risks. These guidelines draw upon thorough literature review (Moustafa, Bello, and Maurushat, 2021) and integrate key factors identified in the study

1. ***Implementing Social Cognitive Theory***: Luszczynska and Schwarzer (2015) propose the use of Social Cognitive Theory (SCT) as a conceptual framework for anticipating and comprehending cybersecurity behaviors. They recommend that training programs should bolster self-efficacy, exemplify desired behaviors, and facilitate vicarious learning
2. ***Hands-on, Practical Training:*** Echoing Wilcox and Bhattacharya (2016), training must include practical simulations, not just theory, to deepen employees' grasp of everyday security challenges.
3. ***Customizing Training to User Needs***: Zulkurnain *et al*. (2015) emphasize tailoring training to individual capabilities and roles, acknowledging user characteristics' impact on social engineering judgment.
4. ***Cultivating a Culture of Security***: Li et al. (2019) emphasize the development of an organizational culture in which cybersecurity becomes a shared responsibility, fostering a collective commitment to safeguarding information
5. ***Encouraging Continuous Learning***: Cybersecurity awareness requires ongoing education, including updates on emerging threats (Mouheb *et al*., 2019).
6. ***Prioritizing Management Support***: Senior management's commitment is pivotal for fostering cybersecurity awareness and compliance
7. ***Incorporating Behavioural Change Techniques***: Pfleeger and Caputo (2012) recommend utilizing effective behavioural change strategies, including performance feedback, goal-setting, and rewards.
8. ***Engaging and Interactive Training***: Engaging training methods like gamification and simulations to enhance learning retention are advocated

6.6 Validation and Corroboration of Findings

The study employed triangulation, combining survey analysis, simulated attacks, and literature review to validate findings on cybersecurity training. Surveys revealed insights into training distribution, participant feedback provided context, and simulated attacks showed significant post-training behavioral improvements,

reducing vulnerability to social engineering. The comprehensive approach, supported by relevant literature, yielded reliable outcomes, thoroughly assessing the effectiveness of cybersecurity training in countering social engineering risks.

6.7 Interpretation of Research Outcomes

This study emphasizes the impact of cybersecurity training on participants' behavior, confidence, emotional responses, threat perception, and decision-making. Post-training, individuals demonstrated increased confidence, proactive handling of social engineering scenarios, and composed emotional reactions. The findings align with past research emphasizing effective cybersecurity training's knowledge-enhancing ability and the importance of heightened threat awareness.

Personal attributes, such as alertness and diligence, significantly influenced susceptibility to social engineering. Evaluation methods effectively captured subtle behavioral shifts, supporting the need for continuous assessment to reflect cybersecurity behavior complexities. Demographics, including age, education, and technical knowledge, played a crucial role in susceptibility to social engineering, emphasizing the importance of considering these factors in cybersecurity awareness initiatives.

7. Conclusion and Future Work

The results suggest a shift towards more engaging and practical training methods (Beuran et al., 2016), indicated by the preference for interactive formats (Figure 8). Regular updates and inclusion of diverse attack types could reflect the evolving threat landscape, filling current program gaps (Almalki, 2016). Behavioural improvements post-training (Figure 10 and 11) advocate for increased investment in such programs. The study's insights might guide cybersecurity consultants in tailoring training to employees' varied confidence levels, emotional responses, threat perceptions, and decision-making styles (Campbell, 2019; Chong, 2018).

Limitations include a small sample size impacting generalizability, and demographic representation limits. The immediate impact focus did not account for long-term knowledge retention or behaviour evolution. The study's limited scope to specific attack types could have neglected other vulnerabilities (Almalki, 2016).

Subsequent inquiries should scrutinize the enduring impacts of training in digital safeguarding and investigate how demographic factors influence vulnerability to digital incursions. Broader investigations into various social engineering techniques could deepen understanding of these threats (Siddiqi et al., 2022).

This thesis successfully investigated cybersecurity training's effectiveness against social engineering threats, aligning theoretical insights with practical applications. Identified gaps were bridged, suggesting continuous improvement in cybersecurity behaviour measurement and demographic factor understanding. The artifact developed has practical implications for diverse organizations.

The limitations identified set the stage for future research, emphasizing the necessity of long-term studies and broader attack scope investigations. This research journey underscores the critical role of continuous advancement in cybersecurity awareness training to combat evolving threats, contributing valuable knowledge and practical guidance to the field.

References

Albladi, S.M. and Weir, G.R., 2018. User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), pp.1-24.

Aldawood, H. and Skinner, G., 2018, December. Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)* (pp. 62-68). IEEE.

Aldawood, H. and Skinner, G., 2019, May. Challenges of implementing training and awareness programs targeting cyber security social engineering. In *2019 cybersecurity and cyberforensics conference (ccc)* (pp. 111-117). IEEE.

Aldawood, H. and Skinner, G., 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), p.73.

Aldawood, H. and Skinner, G., 2020. Analysis and findings of social engineering industry experts' explorative interviews: perspectives on measures, tools, and solutions. *IEEE Access*, *8*, pp.67321-67329.

Alharthi, D.N. and Regan, A.C., 2020. Social engineering defense mechanisms: A taxonomy and a survey of employees' awareness level. In *Intelligent Computing: Proceedings of the 2020 Computing Conference, Volume 1* (pp. 521-541). Springer International Publishing.

Almalki, S., 2016. Integrating Quantitative and Qualitative Data in Mixed Methods Research--Challenges and Benefits. *Journal of education and learning*, *5*(3), pp.288-296.

Arabia-Obedoza, M.R., Rodriguez, G., Johnston, A., Salahdine, F. and Kaabouch, N., 2020, October. Social engineering attacks a reconnaissance synthesis analysis. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0843-0848). IEEE.

Arachchilage, N.A.G. and Love, S., 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, pp.304-312.

Bada, M., Sasse, A.M. and Nurse, J.R., 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bernier, C., 2020. *Evaluating the Effectiveness of Deterrents and Training Methods to Decrease Effectiveness of Social Engineering on Corporate Users Within Large Insurance Providers* (Doctoral dissertation, Northcentral University).

Beuran, R., Chinen, K.I., Tan, Y. and Shinoda, Y., 2016. Towards effective cybersecurity education and training.

Beyer, R.E. and Brummel, B., 2015. Implementing effective cyber security training for end users of computer networks. *Society for Human Resource Management and Society for Industrial and Organizational Psychology*.

Campbell, C.C., 2019. Solutions for counteracting human deception in social engineering attacks. *Information Technology & People*, *32*(5), pp.1130-1152.

Chong, R.C., 2018. *The relationships of social cognitive career theory factors and cybersecurity research self-efficacy* (Doctoral dissertation, Purdue University).

Chowdhury, N. and Gkioulos, V., 2021. Cyber security training for critical infrastructure protection: A

literature review. *Computer Science Review*, *40*, p.100361.

Creswell, J.W. and Creswell, J.D., 2017. *Research design: Qualitative, quantitative, and mixed methods approach*. Sage publications.

Crossler, R.E., Long, J.H., Loraas, T.M. and Trinkle, B.S., 2014. Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), pp.209-226.

Dabke, V., Gadgil, D.G. and Dabke, Y., 2023. Social Engineering as a Driving Force for Innovation in Cybersecurity.

Fan, W., Kevin, L. and Rong, R., 2017. Social engineering: IE based model of human weakness for attack and defense investigations. *IJ Computer Network and Information Security*, *9*(1), pp.1-11.

Ghafir, I., Prenosil, V., Alhejailan, A. and Hammoudeh, M., 2016, August. Social engineering attack strategies and defence approaches. In *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)* (pp. 145-149). IEEE.

Hove, L., 2020. *Strategies Used to Mitigate Social Engineering Attacks* (Doctoral dissertation, Walden University).

Kävrestad, J. and Nohlberg, M., 2021. Evaluation strategies for cybersecurity training methods: a literature review. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15* (pp. 102-112). Springer International Publishing.

Kim, E. and Beuran, R., 2018, October. On designing a cybersecurity educational program for higher education. In *Proceedings of the 10th International Conference on Education Technology and Computers* (pp. 195-200).

Klimburg-Witjes, N. and Wentland, A., 2021. Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses. *Science, Technology, & Human Values*, *46*(6), pp.1316-1339.

Koutsouris, N., Vassilakis, C. and Kolokotronis, N., 2021, July. Cyber-security training evaluation metrics. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 192-197). IEEE.

Koyun, A. and Al Janabi, E., 2017. Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, *4*(6), pp.7533-7538.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E., 2015. Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, pp.113-122.

McAlaney, J. and Benson, V., 2020. Cybersecurity as a social phenomenon. In *Cyber influence and cognitive threats* (pp. 1-8). Academic Press.

Mouheb, D., Abbas, S. and Merabti, M., 2019. Cybersecurity curriculum design: A survey. *Transactions on Edutainment XV*, pp.93-107.

Moustafa, A.A., Bello, A. and Maurushat, A., 2021. The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, p.561011.

Mouton, F., Malan, M.M., Leenen, L. and Venter, H.S., 2014, August. Social engineering attack

framework. In *2014 Information Security for South Africa* (pp. 1-9). IEEE.

Osuagwu, E.U., Chukwudebe, G.A., Salihu, T. and Chukwudebe, V.N., 2015, November. Mitigating social engineering for improved cybersecurity. In *2015 International Conference on Cyberspace (CYBER-Abuja)* (pp. 91-100). IEEE.

Rains, T., 2020. *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd.

Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. *Future internet*, *11*(4), p.89.

Saleem, J. and Hammoudeh, M., 2018. Defense methods against social engineering attacks. *Computer and network security essentials*, pp.603-618.

Santos, H., Pereira, T. and Mendes, I., 2017, March. Challenges and reflections in designing cyber security curriculum. In *2017 IEEE World Engineering Education Conference (EDUNINE)* (pp. 47-51). IEEE.

Siddiqi, M.A., Pak, W. and Siddiqi, M.A., 2022. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), p.6042.

Sobkowicz, P., 2019. Social simulation models at the ethical crossroads. *Science and Engineering Ethics*, *25*(1), pp.143-157.

Spinapolice, M., 2011. Mitigating the risk of social engineering attacks.

Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R. and Ibrahim, M.A., 2022. Social engineering attacks prevention: A systematic literature review. *IEEE Access*, *10*, pp.39325-39343.

Torten, R., Reaiche, C. and Boyle, S., 2018. The impact of security awareness on information technology professionals' behavior. *Computers & Security*, *79*, pp.68-79.

Vance, A., Siponen, M. and Pahnila, S., 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), pp.190-198.

Wang, Z., Sun, L. and Zhu, H., 2020. Defining social engineering in cybersecurity. *IEEE Access*, *8*, pp.85094-85115.

Washo, A.H., 2021. An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*, p.100126.

Wilcox, H. and Bhattacharya, M., 2016, June. A framework to mitigate social engineering through social media within the enterprise. In *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)* (pp. 1039-1044). IEEE.

Yamin, M.M. and Katt, B., 2019, August. Cyber security skill set analysis for common curricula development. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-8).

Zulkurnain, A.U., Hamidy, A.K.B.K., Husain, A.B. and Chizari, H., 2015. Social engineering attack mitigation. *International Journal of Mathematics and Computational Science*, *1*(4), pp.188-198