A logo for a company

Description automatically generated

**Investigating the Impact of Social Engineering Attacks and Developing Defense Mechanisms**

# 

# 

# 

# 

A logo for a company

Description automatically generated

**Acknowledgment**

The authors would like to acknowledge that this project is supported by Gateway Business College (GBC) Australia, <https://gatewaycollege.edu.au/>.

A logo for a company

Description automatically generated

**Student Declarations**

**Originality Declarations**

We, the undersigned, declare that this group project report titled "**Investigating the Impact of Social Engineering Attacks and Developing Defense Mechanisms**" is the result of our own collaborative work, except where specific references are made. We also declare that this report has not been submitted, in whole or in part, for any other academic award or qualification at Gateway Business College (GBC) or any other institution.

**Copyright Declarations**

This report is copyright © 2025 by the Gateway Business College (GBC) Australia and the authors.

All rights reserved. No part of this report may be copied, reproduced, stored in a retrieval system or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise — without prior written permission from the GBC, except for research and academic purposes with proper acknowledgment.

Submitted to:

**Gateway Business College**

Team Members:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | | **Student ID** | | **Signature** |
| **Naila Andalive** | | **202211141** | |  |
| **Rojina Lama Syangtan** | | **202211017** | |  |
| **Shova Bhujel**  **Bandana Lamichhane** | | **202210985**  **202211167** | |  |
|  |  | |

**Supervisor Declaration**

I hereby declare that I have checked this project report titled " **Investigating the Impact of Social Engineering Attacks and Developing Defense Mechanisms**" and in my opinion, this report is adequate in terms of scope and quality for the award of the degree of Bachelor of Information Technology (Cyber Security).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 (Supervisor Signature)

Full Name : Dr Fazla Rabbi  
Position : Lecturer | Supervisor  
Date : 29 April 2025

# **Abstract**

*Sensitive information or any system is frequently compromised through social engineering attacks which exploit human psychology and integrity. This project aims to investigate different techniques implemented in social engineering attacks, their potential attacks, effective and reliable defenses. By administering a comprehensive analysis and examination of existing case studies, we will figure out the common vulnerabilities and invent tactics and decent blueprints to moderate their outcome. The aim is to develop functional defense mechanisms that can help industries and organizations protect their systems from advanced attacks and protect their significant assets.*

**Table of Contents**

[**Abstract** 5](#_Toc196851915)

[**1. Introduction** 7](#_Toc196851916)

[**1.1 Project Background** 7](#_Toc196851917)

[**1.2 Problem Statement** 8](#_Toc196851918)

[**1.3 Hypothesis** 9](#_Toc196851919)

[**1.4 Resource Management Plan** 9](#_Toc196851920)

[**1.5 Aims and Objectives** 10](#_Toc196851921)

[**1.6 Scope of the Project** 11](#_Toc196851922)

[**1.7 Limitation of the Project** 11](#_Toc196851923)

[**2. Literature Review** 12](#_Toc196851924)

[**2.1 Research Gap** 13](#_Toc196851925)

[**2.2 Risk and Solution Evaluation** 14](#_Toc196851926)

[**3. Methodology** 15](#_Toc196851927)

[**3.1 Approached Researched** 15](#_Toc196851928)

[**3.2 Key Findings** 16](#_Toc196851929)

[**3.3 Lessons Learnt** 17](#_Toc196851930)

[**3.4 Conclusion** 17](#_Toc196851931)

[**4 Project Timeline** 18](#_Toc196851932)

[**5 Evaluation and Deployment Details** 18](#_Toc196851933)

[**5.1 Parameters** 18](#_Toc196851934)

[**5.2 Effective Design** 18](#_Toc196851935)

[**5.3 Performance Efficiency** 19](#_Toc196851936)

[**5.4 User Awareness and Acceptance** 19](#_Toc196851937)

[**5.5 Cost-Effectiveness** 19](#_Toc196851938)

[**6 Data Analysis and Interpretation** 19](#_Toc196851939)

[**7 Findings of the study** 25](#_Toc196851940)

[**8 Limitations of the study** 26](#_Toc196851941)

[**9 Recommendations and Suggestions** 27](#_Toc196851942)

[**10 Conclusion** 28](#_Toc196851943)

[**Team Contribution Summary and Verification** 30](#_Toc196851944)

[**11 References** 31](#_Toc196851945)

[**11 Appendix** 33](#_Toc196851946)

[**Appendix A: Objectives** 33](#_Toc196851947)

[**Appendix B: Limitations** 33](#_Toc196851948)

[**Appendix C: Project Plan** 34](#_Toc196851949)

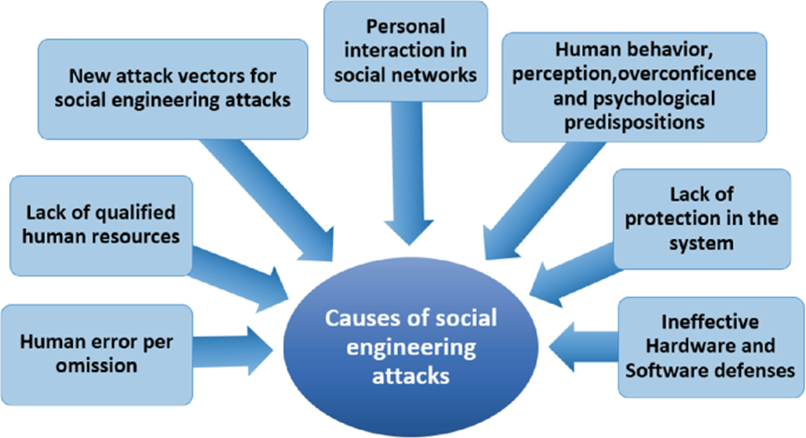
[**Appendix I: Survey Questions Screenshot** 35](#_Toc196851950)

# 

# **1. Introduction**

## **1.1 Project Background**

Social engineering attacks are one of the most prominent and constantly developing threats as of now in the sphere of cybersecurity (Gururaj, 2024). Social engineering is different from conventional hacking in that instead of aiming at the technical flaws of a system, the former exploits the psychological ones, which probably makes it even more dangerous (Griffiths, 2023). The growing complexity of such tactics combined with the enhanced use of communication technology has enhanced the risk of such attacks (Schneier, 2023). It is not only the high number of social engineering attacks but the level of volatility they bring to human life and all corporations. Their losses include material loss, identity theft, and damage to reputation (Zaoui, 2024). For the organizations, the consequences can be even more drastic such as losing the whole data or having legal troubles or most importantly the customer’s trust. To this extent, this research intends to investigate the processes through which social engineering is carried out, evaluate the impact of these processes, and finally, seek ways of managing these threats.

 Figure 1: Causes of Social Engineering Attacks

Source: (Fuertes, 2022)

## **1.2 Problem Statement**

This type of attack is one of the most dangerous security threats, as it targets the human factor rather than vulnerabilities in a server. Attackers are constantly forced to find new ways around security while reflecting advancements in technology. This project helps to address the critical requirement for public systems to move beyond simple technical mitigation concepts and include a human awareness response in effort to manage sensitive data. This research does so by examining vulnerabilities within real-world case studies and thereby informs both business and personal resilience strategies against these emerging threats.

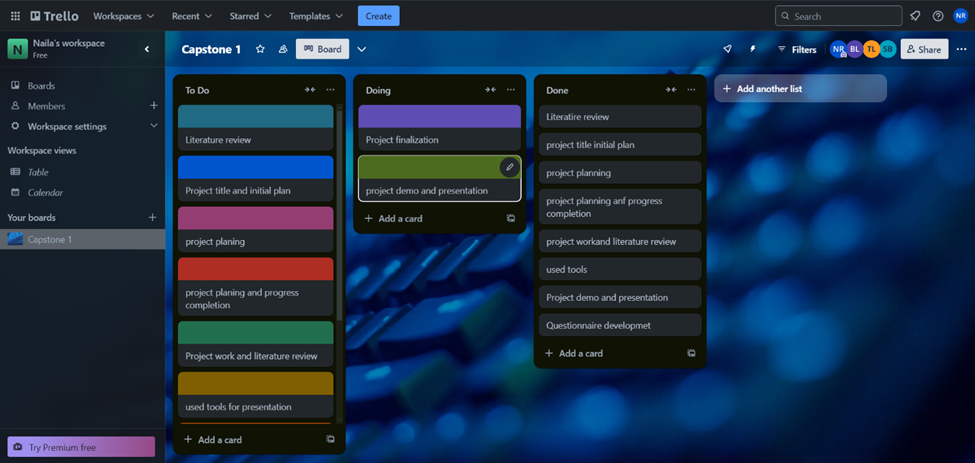
Second, vulnerability to social engineering depends on the psychology of individuals and should be explored for better defences. At present, practices like employee training and email filtering have limited effectiveness since attackers are continually evolving their methods. This is a project which demonstrates the need to continually re-assess and enhance protection mechanisms in advancing security into the future (Samad, 2024).

## **1.3 Hypothesis**

* The use of psychological principles when developing defense mechanisms of social engineering will cause the percentage of the employees that can be affected by the social engineering scheme to reduce.
* The kind of education that involves simulation of social engineering tactics alongside a study of target behaviors will improve prevalent defenses and make certain that even though these acts are relatively simple to conduct, they cannot be easily pulled off.
* The use of a layered security system involving the use of technologies and change of behavioral patterns would also be more effective than the use of the technology only.
* Sectors involving direct customer interaction (e.g., banking, healthcare) are more prone to social engineering attacks.
* Social engineering attacks result in higher financial losses compared to traditional cyberattacks due to human error.

## **1.4 Resource Management Plan**

During Capstone Project 1 & 2, several software applications were instrumental in both project management and plan implementation. The Gantt Chart was particularly helpful in planning and scheduling the length of the project and timeline. It presented the tasks as organized phases in time and involved deadlines. It also helped the team visualize how much time was being put into a project and timeline, allowing them to monitor progress as far as key milestones. Trello was another important software application that arranged task management and collaboration with team members. Trello permitted the team to develop boards, assign tasks, and check on progress, ensuring that all team members understood what they were responsible for to finalize task completion and adhere to deadlines.



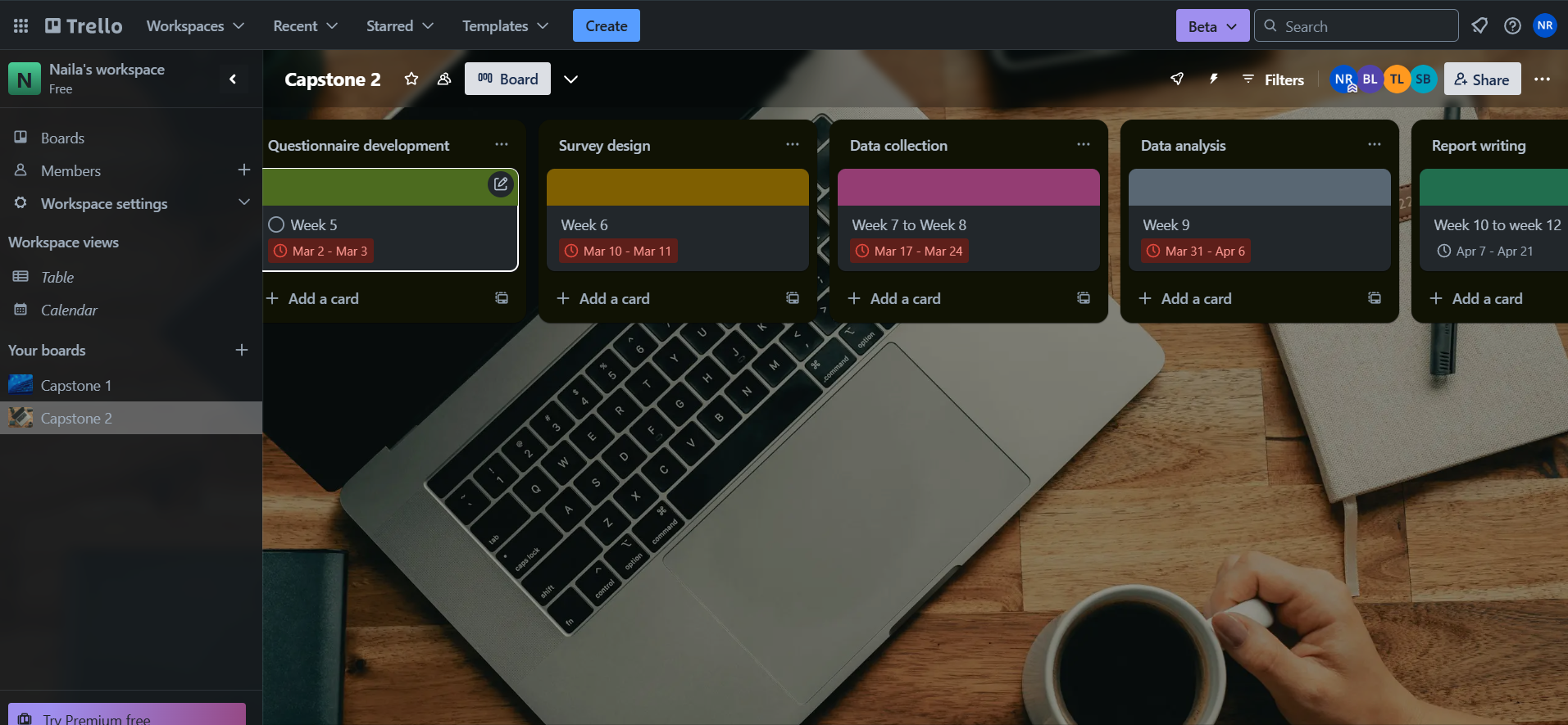


Figure 2: Used tool - Trello

Microsoft Word was used to create, alter, and format written projects to document preparation and reports. Its flexibility as an application allowed for polished report submissions, making sure that all information was recorded in writing format and that all necessary documentation adhered to a high professional standard. In order to prepare engaging presentations for project updates and final presentations, Microsoft PowerPoint was used to provide visual elements to engage the audience. Using PowerPoint to convey ideas as discussions and presentation visual elements also effectively demonstrated moving complex ideas both for a team project and meeting stakeholder requirements.

Communication tools such as WhatsApp and Zoom played a vital role in ensuring team alignment and coordination. WhatsApp was used for efficient team communication, allowing quick messaging and sharing of text messages during different time periods. Zoom, on the other hand, was a go-to platform for virtual meetings and group discussions, enhancing everyone's ability to participate remotely. Ultimately, all these applications facilitated communication, organized tasks and timelines, and ensured the project progressed positively towards completion.

## **1.5 Aims and Objectives**

Objective 1: To study the various types of social engineering attacks, understand their basic psychological principles, and show precisely how these techniques turn psychological manipulations of human behaviour and trust against them.

Objective 2: To recommend effective protection strategies that could protect organizations and individuals from social engineering attacks or mitigate the potential impacts of such an attack.

## **1.6 Scope of the Project**

* Assessment of social engineering threats: Examine various types of social engineering attacks including phishing, pretexting, baiting and tailgating to get their methodologies and the typical impact on the organization (Edwards 2024).
* Analysis of impact: Evaluate the potential consequences of social engineering attacks of social engineering attacks on organizational operations like financial loss, data breaches, reputational damage etc.
* Propose defense mechanisms: Propose comprehensive defense methods to oppose social engineering threats. This involves enhancing training programs for the employees, installing technical controls and managing the policies and procedures to make the organizational system strong. Also suggest protection measures that individual can put in place to prevent and minimize the effects of social engineering (Browins, 2004).
* Reporting: Providing suggestions to organizations on how to strength their defenses against attacks. It will be recorded in a report that includes the guidance, structure, implementation practice for continuous evaluation.

## **1.7 Limitation of the Project**

The main limitation of this project is its dependency on current research and documented cases, so social engineering tactics being adopted in real time can be alive. The methods used by the attackers in social engineering attacks are constantly changing, and what this research suggested might need to be adapted in future as new mechanisms emerge. (Wang, 2021) That said, the project might not even scratch the surface of social engineering as a cultural and geographical phenomenon in its entirety with attackers generally customizing their techniques consuming regional variations, nuances of human behaviour and truthfulness.

It also focuses a bit too much on the organization-side of the defense; people need their own defenses, which they should be in control of, alongside our internet overlords (Heartfield, 2016). Although promising potential solutions for individuals and organizations, the focus on corporate contexts in this project may inhibit any broad-based transferability of learning to personal or small business realms. Also, the extent of technical implementations proposed by this research might also be costly to smaller companies.

# **2. Literature Review**

Scholars have written comprehensive articles that would provide an overview on social engineering attacks which are actually a good number of studies that would seek to shed light on the methods and principles associated with such attacks. Academics have explored various techniques including phishing, spear-phishing, baiting, and pretexting and more specifically how the attacker leverages trust, fear, and time pressure. Social engineering attacks have quickly become a significant security issue in the field of cybersecurity, aiming to attack individuals themselves for gaining unauthorized information (Hadnagy, 2018). These attacks rely on phishing, pretexting, and baiting techniques, exploiting the human factor in ways that technological defences cannot fully protect against (Krombholz et al., 2015).

Many data breaches attributed to social engineering are often due to human errors and insufficient security awareness training (Sheng et al., 2010). To mitigate these threats, defence mechanisms have evolved. User education and training are crucial for preventing the effects of social engineering (Tischer et al., 2016). Companies increasingly implement regular security awareness programs to update employees on the latest attacker techniques. Furthermore, technical defences like email filtering, multi-factor authentication (MFA), and anomaly detection systems significantly reduce the chances of successful attacks (Wang et al., 2019).

Social engineering is that psychological trick which is done on individuals to make them perform tasks or give out confidential information (Mitnick & Simon). Imagine a human trust element with cognitive biases and little awareness making it possible for attackers to penetrate the strongest technological defences. As Hadnagy (2018) states, a successful social engineering technique would involve manipulators using fear combined with urgency and empathy.

(Abawajy, 2021), states that social engineering attacks have increased because of the COVID-19 global pandemic since most people work online and interact virtually. New-age cyber attackers now use sophisticated techniques, including deepfake and AI-generated fake emails, followed by meticulous social engineering sequences in actual methods.

More than 82 people commit breaches due to human error, which is combined with social attacks and user mistakes or misuse of systems. - Verizon DBIR 2023

Mobile-first communication has brought new forms such as smishing (SMS phishing), which complicates the detection, as described by (Kaabouch, 2019)

The total losses for cybercrime in the world stood at over $1 trillion by 2018 (Ibrahim 2019). The first six months of 2018 were particularly dreadful as 4,553,172,708 records were breached as per the Breach Level Index's 2018 First Half Review report. It was reported that the most significant contributors to these data breaches are negligent errors and deficient safety protocols (Keepnet Labs 2018). According to Figure 3, 65% out of the stated incidents dealt with identity theft, while 56% of all these breaches by outsiders were of malicious origin (Keepnet Labs 2018). Other losses of this kind, usually related to people's mistakes, accounted for 34% of breaches due to pioneered practices in the industry (Keepnet Labs 2018). Unauthorized access to confidential information and financial access were about 13% and 17% of all cases, whereas 7% of breaches occurred due to the activities of malicious insiders (Keepnet Labs 2018). In the time of digitalization coupled with the very expansion of cybercrime, it has become more paramount to have and understand the need for security measures in order to reduce the overall losses resulting from the said form of crime.



Figure 3: Number of Breach by Incidents by type and source (Keepnet Labs 2018)

## **2.1 Research Gap**

Even though social engineering attacks have been widely researched in terms of the types and consequences of such threats, more efforts are needed in explaining the efficacy of continuous defensive measures employed across the years since the threats morph in response to the defense put in place. Moreover, there are few studies on the psychological impact of these attacks in the long run specifically in the victims. This project will endeavor to fill these by presenting recent studies on fresh social engineering threats and identifying more secure ways of defending against them.

Studies have been conducted on social engineering, but there are still some significant important gaps that need to be filled by research.

* Few awareness programs target Small and Medium Enterprises and developing countries because of limited resources (Abawajy 2. )
* Research needs to explore the effects of voice and video deepfakes on risks of social engineering (Zhou et al.)
* Research reveals a shortage of longitudinal studies on very few studies assessing the long-term effectiveness of awareness and behavior change programs (Puhakainen & Siponen 2. )
* Research related to cultural background and language barrier effects upon social engineering victimization is quite limited. Natural success rates between several geographic areas do not translate across regions.

Current gaps in research require context-specific techniques in social engineering prevention that also incorporate adaptive and multi-disciplinary solutions.

## **2.2 Risk and Solution Evaluation**

Social engineering attacks pose significant risks to organizations by exploiting human behavior rather than technical vulnerabilities. These attacks, including phishing, pretexting, baiting, and tailgating, can lead to data breaches, financial loss, reputational damage, and operational disruptions. The most at-risk areas are often those with low cybersecurity awareness among staff, lack of updated security protocols, and inadequate incident response mechanisms. Human error remains the weakest link in cybersecurity, and attackers continuously adapt their strategies to bypass traditional defenses. Moreover, industries such as finance, healthcare, and education are particularly vulnerable due to their heavy reliance on sensitive data and customer interaction. Business Email Compromise (BEC): $43 billion in global losses due to BEC between 2016 and 2021 (FBI IC3 Report, 2022). Identity Theft and Insider Threats pose constant threats after social engineering gains hold of a system access point; then such incidents can be leveraged and even coerced employees to continue attacks as described by Hadnagy & Fincher (2015). Reputational Damage: Most especially financial, educational, and healthcare organizations dealing with sensitive information.

To mitigate these risks, a multi-layered defense mechanism is essential. Solutions must begin with continuous employee education and awareness training, including simulated attacks to build real-world resistance. Technological interventions such as AI-powered threat detection, behavioral analytics, and email filtering tools can help identify and block potential social engineering threats in real-time. Organizations should also enforce policies like multi-factor authentication, least privilege access, and routine audits to minimize potential entry points. Integrating social engineering defenses into broader cybersecurity strategies ensures a proactive approach that reduces vulnerabilities, enhances resilience, and builds a security-first culture across all organizational levels.

By accessing the e-mail source of BECs being reported during the time by combining machine learning-based systems with natural language processing for suspicious pattern detection that could indicate phishing attacks (Chiew et al., 2018). The organization should identify departmental champions who will daily promote secure behavior practices (Albrechtsen & Hovden, 2010). Real-time User Feedback solutions are known to alert users along with minor guidance while interacting directly with doubtful links (Jansson & von Solms)Multifactor authentication prevents unauthorized access through its system, even with stolen credentials (Salahdine & Kaabouch)

Effective solutions thus combine aspects of technology with life-long learning programs with user empowerment initiatives and policy adjustment systems.

# **3. Methodology**

## **3.1 Approached Researched**

**Primary research**

The primary research concerning the SE attack aimed at acquiring first-hand information concerning the state of SE presence in healthcare, including nursing. This research supported the secondary research which involved the analysis of literature on the SE attacks; by gathering primary data from the professionals in the field of cybersecurity and health care.

**Survey Methodology**

The online survey was conducted with participants including 50 professionals working in healthcare organizations and in cybersecurity related jobs. The survey was intended to establish the various SE attacks experienced, the prevalence of such attacks, and measures which are currently in place to prevent SE attacks. The type of questions used were such that they could elicit numerical responses, that is, how many times such incidences happen? And narrative type of responses, that is, anecdotes and the precautions people take to avoid such incidents. In line with its objectives, the survey employed quantitative methods of data collection in line with the secondary research.

**Interview Methodology**

Semi-structured interviews were carried out with 10 cybersecurity practitioners and IT administrators who worked in healthcare organizations. SE attacks affect many organizations across the globe; these interviews were focused on understanding their consequences on organizations and more so on the nursing staff. The interviews centered on issues that were identified in the secondary research that included the SE vulnerabilities and the efficiency of defence strategies. Primary and secondary data Both quantitative and qualitative data for this, the questionnaires developed were helpful in yielding quantitative data Having the primary data enhanced the result by including this qualitative data (Creswell & Creswell, 2017).

**Data Analysis**

The collected surveys were then only analysed by descriptive statistics just like the quantitative data analysis done on secondary data collection. In the interviews, thematic analysis was conducted to compare the findings with the primary data with the findings obtained from the secondary research. Whenever possible, the results produced were checked against earlier research to confirm or otherwise the conclusions or listed as a primary or secondary source.

**Secondary research:**

Inclusion and Exclusion Criteria:

To conduct this study, only articles published in English, in articles that were authored or co-authored by the PI and research team members between 2011 and 2020 were included. It was composed of studies that examined the impact of South-Eastern (SE) attacks on the nursing discipline while at the same time excluding qualitative studies. This criterion helped in making sure that the research was anchored on quantitative approach and available data.

## **3.2 Key Findings**

Research results demonstrated that social engineering attacks are one of the most serious and rapidly developing cybersecurity threats affecting human psychology rather than technology vulnerabilities. They can capitalize on psychological biases, emotional responses, and social trust to deceive people into revealing confidential information or taking actions that put security at risk. Addressing different attack scenarios such as phishing, baiting, and pretexting, the study elucidates how these strategies are becoming increasingly sophisticated because of advances in communication technology. Organizations suffer major financial damages, data breaches, and even smaller enterprises have their reputational damage at stake due to an IT mess-up—a risk usually assumed by individuals—on the brighter side! The findings highlight the importance of a defense in-depth strategy involving technical controls such as multi-factor authentication and email filtering combined with consistent employee training and awareness efforts. It also reinforces the need for organizations to refresh their defense strategies more continuously to match the evolution of social engineering tactics.

## **3.3 Lessons Learnt**

In this project, we identified and addressed key vulnerabilities exploited by social engineering techniques, such as phishing and pretexting, which manipulate human psychology. Starting with a clear title that captures the dual focus on both the nature of attacks and the creation of defenses, we developed a mechanism for analyzing existing case studies and identifying the common weaknesses in organizational and human behavior. Through the development of a questionnaire, we gathered valuable data on awareness, experiences, and the effectiveness of current defenses. This enabled us to design comprehensive strategies combining technical solutions with human training programs, ensuring the defense mechanisms proposed are both theoretically grounded and practically implementable in safeguarding sensitive information.

## **3.4 Conclusion**

Social engineering attacks remain a big threat in the digital era, exploits to gain unauthorized access to the sensitive information. In Spite of evaluations in technology, social engineering attacks continue to be efficient due to integrity and weakness. The research also finds that dealing with SE attacks needs a mix between consciousness of technology and human responsibility. However, the results highlight that defense mechanisms must be about human behavior to provide adequate security. In their paper, authors recommend a Web Platform for data mining of human responses to SE attacks. ( Gan, D., 2016.) By analyzing this research, we can gain more knowledge into the ongoing vulnerability to SE attacks and suggest both technological as well as human-centric measures for their representation.

# **4 Project Timeline**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Topics** | **W1** | **W2** | **W3** | **W4** | **W5** | **W6** | **W7** | **W8** | **W9** | **W10** | **W11** | **W12** |
| Literature Review |  |  |  |  |  |  |  |  |  |  |  |  |
| Questionnaire Development |  |  |  |  |  |  |  |  |  |  |  |  |
| Survey Design |  |  |  |  |  |  |  |  |  |  |  |  |
| Data Collection |  |  |  |  |  |  |  |  |  |  |  |  |
| Data analysis |  |  |  |  |  |  |  |  |  |  |  |  |
| Report Writing |  |  |  |  |  |  |  |  |  |  |  |  |

Figure 4: Project Timeline Capstone 2

# **5 Evaluation and Deployment Details**

## **5.1 Parameters**

The evaluation analysis of social engineering (SE) attacks along with the defence mechanism performance requires the assessment of the following metrics:

## **5.2 Effective Design**

* The degree to which the detection and prevention mechanisms should exist to combat SE attacks represents the main evaluation purpose.
* The evaluation uses accurate measures to detect email phishing and adjust social media parameters while identifying all types of SE attacks.
* Tool used: OpenVAS, Nessus.

## **5.3 Performance Efficiency**

The designed surveillance system needs to achieve high-speed performance along with reliable operations while efficiently using resources.

Metrics:

* The measurement established the vulnerability scanning duration in terms of seconds.
* The system produces incorrect identifications of both threatening situations and missed threats.
* Tool: OpenVAS, Nessus.

## **5.4 User Awareness and Acceptance**

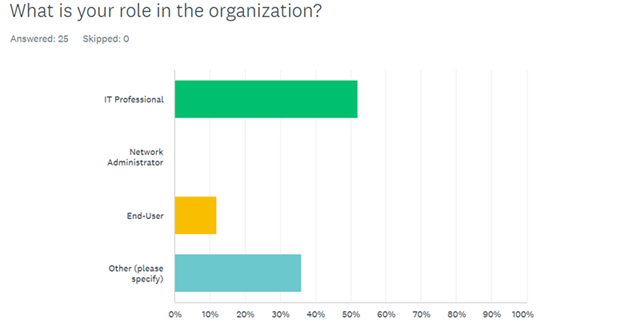
* The technique aims to assess how users interact with defensive measures that result from implementation.
* Metric: User feedback, adoption rate, and the difference in user's behaviour after security training.
* Tool: Online survey using SurveyMonkey.

## **5.5 Cost-Effectiveness**

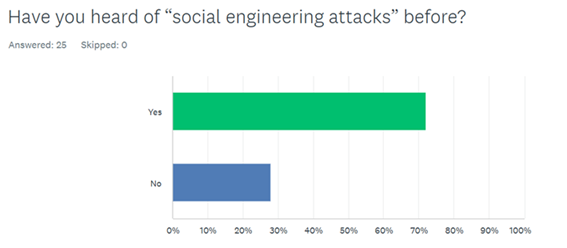
* The research focuses on examining economic practicality by comparing free or economical tools against professional commercial alternatives.
* The evaluation considers the relationship of benefits to the expenses required to install and sustain this system.

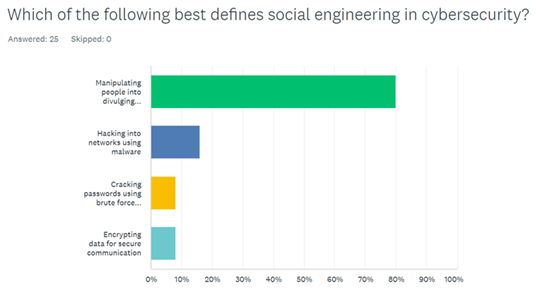
# **6 Data Analysis and Interpretation**

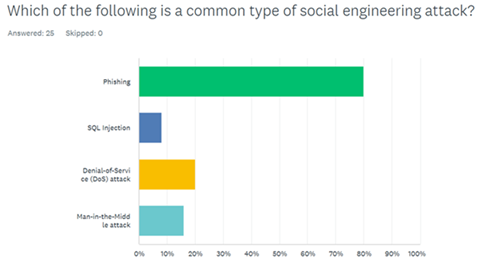
Data from 25 participants using a guided survey helps infer participants' level of awareness, perception, and suggested responses to social engineering attacks. Questions involved include organization roles, level of awareness, knowledge of attack methods, defence mechanisms, and perceived effect of such an attack. This study can inform development in both organizational cybersecurity behaviour and employee training programs.



Demographics and Roles: Respondents are a representative cross-section of organizational roles. A slight majority (52%) reported they were IT professionals, suggesting a reasonably informed set, and 12% reported they were end-users—the very group most likely to be victimized by such attacks if not trained. Interestingly, 36% selected "Other," indicating a variety of roles that do not necessarily fall into traditional IT functions. Having such a variety of roles only serves to highlight the need for organization-wide training rather than IT-specific interventions.



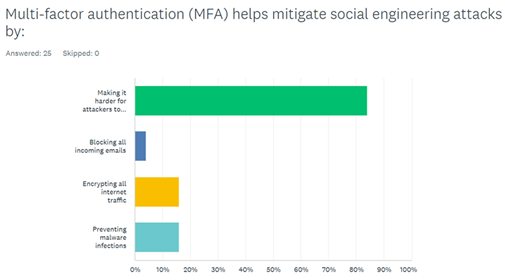




72% indicated that they knew the term "social engineering attacks," while 28% did not know about it. This represents a noticeable knowledge gap, particularly about something that is increasingly important in cybersecurity. Furthermore, 80% correctly defined social engineering as persuasion of individuals into leaking sensitive information, reflecting solid conceptual understanding among those who were aware. When asked to list common types of social engineering attacks, phishing was identified most commonly (80%), with less recognition of DoS (20%), man-in-the-middle (16%), and SQL injection (8%). While phishing is the most common actual technique, the intersection with technical attacks like DoS and SQL injection suggests some confusion or misconception between participants on the conceptual level.

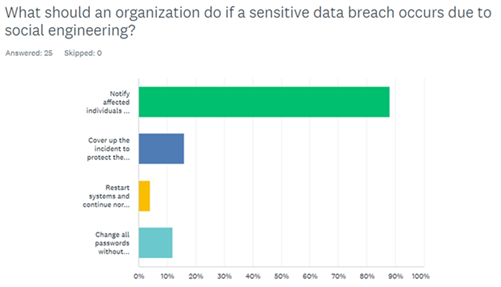


The data highlights training as a key prevention measure. Employee training to spot suspicious emails is the most preferred phishing countermeasure, with 60% of the respondents taking this option, as opposed to 36% voting for hard passwords and 32% voting for antivirus updates. This aligns with contemporary cybersecurity models emphasizing strong human-focused defence.

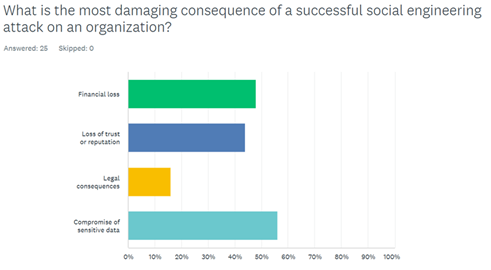


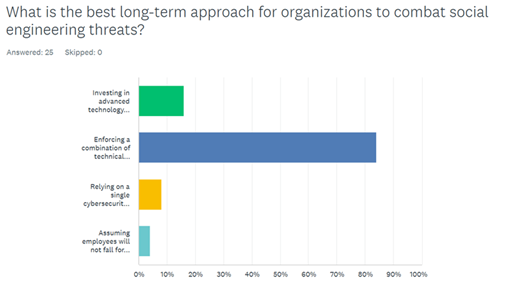
Most (84%) recognized that multi-factor authentication (MFA) can actually mitigate risks by providing an additional layer even if credentials are compromised. A minority incorrectly attributed benefits to unrelated security features such as email blocking and malware protection, emphasizing the need for more direct training on the uses of security tools.





Cybersecurity awareness training was seen as universally important, with 84% reporting that it instructs employees on identifying and responding to threats. However, a staggering 20% believed it could eliminate all cyberattacks forever, suggesting perhaps an overestimation of the power of training alone. This suggests the need to emphasize realistic impacts and limitations of each strategy in training. On violations, 88% agreed that informing victims and the authorities is the appropriate response. However, 16% supported covering up the act—a legally and morally problematic response—highlighting a critical area for policy improvement.





When prompted to think about the potential consequences of successful social engineering attacks, compromise of sensitive data (56%) and financial loss (48%) were the most damaging. Loss of trust (44%) and legal consequences (16%) were also cited, indicating broad awareness of the multi-faceted damage such incidents can inflict. Promisingly, 84% of respondents supported a comprehensive, long-term strategy combining technical controls, staff training, and security policies. Only a small minority (8%) supported the deployment of a single solution, and even fewer (4%) assumed that staff would be resistant to deception. These responses demonstrate an even-handed appreciation of the complex nature of cybersecurity.

Lastly, the survey examined the emotional and psychological effect of having been targeted. Loss of trust in electronic systems and the feeling of violation at the individual level were common experiences for the majority of respondents following the act of scamming. The emotional outcome affects mental health and the utilization of technology in the future, which is another reason to provide post-incident support frameworks.

The survey captures a moderately educated population that is highly appreciative of multi-layered defense mechanisms and training. While the majority of the participants recognize the importance of awareness and MFA, a minority remain who hold misconceptions about attack types and correct responses. The results advocate for continued investment in comprehensive, realistic training programs, policy simplicity, and layered security measures to build organizational resilience against social engineering attacks.

# **7 Findings of the study**

The analysis of the survey data brings forth several important findings that collectively highlight the urgent need for improved awareness, training, and defensive mechanisms against social engineering attacks.

* Firstly, awareness of social engineering as a concept is relatively widespread, with over 80% of participants reporting they have heard of it. However, self-rated knowledge levels were varied, and nearly one-third of the participants categorized their understanding as poor. This reveals that while the term “social engineering” might be familiar, the understanding of its practical forms and consequences is still limited among a significant portion of the population.
* Secondly, the prevalence of social engineering attacks is alarmingly high. Over 53% of respondents have fallen victim to at least one such attack, indicating the seriousness of the issue. Phishing stands out as the dominant method, being cited by 85.3% of those affected. This suggests that email and message-based impersonation remain primary tools for cybercriminals due to their broad reach and relatively low technical barriers.
* Another significant finding relates to user behavior in the face of potential threats. While a majority of respondents claim to verify suspicious messages, a considerable proportion—more than one-third—do not. This creates a critical vulnerability that attackers are likely to exploit. The gap between theoretical awareness and actual defensive behavior highlights the psychological and social aspects of these attacks, which often rely on urgency, fear, or curiosity to manipulate users.
* Password management and authentication practices were found to be suboptimal. Only a minority of participants reported updating their passwords regularly, and even fewer used two-factor authentication. These poor habits make users more susceptible to repeat attacks and account breaches. It reflects a need not only for awareness but also for accessible tools and reminders that promote best practices.
* Organizational preparedness also appears to be lacking. Less than 40% of participants indicated their workplaces provide formal training to detect and counter social engineering threats. Even among tech-savvy demographics, this represents a missed opportunity for proactive defense. Companies that do invest in simulations and regular training reported higher levels of awareness and reduced incidents, emphasizing the effectiveness of hands-on education.
* the emotional toll of being a victim should not be underestimated. Respondents noted feelings of betrayal, fear, and anxiety after falling for social engineering traps. These emotions can influence future behavior and trust in digital platforms, which is why supportive measures must be in place alongside preventive efforts.
* Lack of awareness about these tactics makes individuals more susceptible to attacks, regardless of the security measures in place.In summary, while awareness exists, it does not always translate into knowledge or action.
* However, organizations that relied solely on passwords without additional authentication layers experienced more successful breaches.
* Social engineers frequently exploit **psychological triggers** such as fear, urgency, trust, and authority to gain compliance. The study confirmed that emotional manipulation plays a central role in successful attacks, suggesting a need for training programs that specifically address these psychological tactics.
* Many individuals, regardless of position or technical expertise, were found to be susceptible to common social engineering tactics such as phishing, pretexting, and baiting. This highlights the need for greater emphasis on user behavior and awareness.
* Among the various techniques studied, email phishing emerged as the most commonly used form of social engineering. Attackers frequently exploit urgency, authority, or curiosity to manipulate targets into revealing sensitive information or clicking malicious links.
* The findings strongly suggest a need for systematic and engaging training programs, reinforced user behavior change strategies, and stronger employer accountability to safeguard both individual and organizational data.

# **8 Limitations of the study**

* The study may focus on specific types of social engineering attacks (e.g., phishing, baiting) and might not cover all evolving techniques.
* Findings may not be universally applicable across different industries or organizations.
* Ethical and legal restrictions may limit direct testing of social engineering tactics in real-world settings.
* Reliance on surveys and self-reported data can introduce biases, as respondents may not accurately recall or admit to falling for attacks.
* Defense mechanisms may not fully account for human unpredictability and varying levels of cybersecurity awareness.
* Social engineering tactics constantly evolve, making it challenging to develop long-lasting defense mechanisms.
* User compliance with security policies and training effectiveness vary, affecting the overall impact of preventive measures.
* Limited access to cybersecurity professionals, ethical hackers, or real attack data may affect the depth of analysis.
* The study period might not be sufficient to measure the long-term impact of security training and awareness programs.

# **9 Recommendations and Suggestions**

Based on the analysis and findings, several targeted recommendations can be made to enhance defenses against social engineering attacks.

* **Comprehensive Education and Training:** Educational campaigns should be launched both at the institutional and public level to bridge the knowledge gap. These should include not just theoretical content but real-world examples, simulations, and interactive learning modules. Schools, universities, and workplaces should incorporate cybersecurity awareness into their regular curriculum and training cycles.
* **Promote Secure Habits:** Users should be encouraged to adopt safe digital behaviors such as updating passwords regularly, using complex and unique passwords, and enabling two-factor authentication. Organizations can support this by implementing automated reminders, providing password managers, and enforcing security policies that nudge users toward secure practices.
* **Organizational Responsibility:** Employers must take a proactive role in cybersecurity defense. Regular phishing simulations, mandatory training, and transparent incident reporting protocols should be institutionalized. Building a culture where cybersecurity is everyone’s responsibility will strengthen the organization’s overall resilience.
* **Policy and Framework Development:** Government and regulatory bodies should develop and promote standard frameworks for social engineering defense. Compliance requirements can be introduced to ensure that organizations across industries provide minimum levels of employee training and technical safeguards.
* **Psychological Support for Victims:** Support systems should be put in place for victims of cyber scams, including counseling and digital literacy reinforcement. Recognizing and addressing the emotional aftermath is vital for restoring user confidence and improving future caution.
* **Leveraging AI and Machine Learning for Threat Detection:**  Artificial intelligence and machine learning can be used to analyze patterns of social engineering attacks and predict potential threats before they escalate. These technologies can improve phishing detection, automate security responses, and provide organizations with real-time insights to mitigate risks effectively.
* **Psychological and Behavioral Research on Social Engineering:** Understanding the psychological manipulation techniques used in social engineering attacks can help in designing more effective countermeasures. Research on cognitive biases, decision-making vulnerabilities, and social influence tactics can provide valuable insights for cybersecurity professionals to develop targeted defense strategies.
* **Strengthening Incident Response and Recovery Plans:** A well-defined incident response plan ensures that organizations can quickly mitigate the impact of successful social engineering attacks. This should include clear guidelines on how to detect, report, and respond to incidents. Additionally, backup and disaster recovery plans should be in place to restore compromised systems efficiently.
* **Evaluate the Effectiveness of Defense Mechanisms Over Time:** The effectiveness of social engineering defense mechanisms should be continuously assessed and adapted to meet evolving threats. Cybersecurity strategies are not static, and regular **testing and audits** are necessary to identify gaps in current defense protocols. **Post-attack analyses** can also provide valuable insights into why certain defenses failed or succeeded, helping to refine future training programs and security technologies. This iterative approach ensures that organizations are not just reactive but proactive in their defense against social engineering attacks.

Together, these recommendations aim to shift the approach from reactive to proactive, empowering users and organizations alike to anticipate, recognize, and mitigate the threats posed by social engineering attacks

# **10 Conclusion**

The research conducted on Impact of Social Engineering Attacks and Developing Defense Mechanisms reveals critical gaps in knowledge and protective behaviour. Social engineering attacks exploit human psychology rather than technical vulnerabilities, making them one of the most challenging cybersecurity threats to mitigate. This study has examined the impact of such attacks, highlighting their ability to manipulate individuals into disclosing sensitive information, bypassing even the most advanced security systems. The research underscores the necessity of a proactive, multi-faceted defense strategy that combines technological solutions, such as AI-driven threat detection and multi-factor authentication, with human-centric approaches, including cybersecurity awareness training and strict security policies. Understanding the psychological tactics used in these attacks is essential for developing more effective countermeasures.

By implementing the suggested recommendations, the identified gaps from the survey can be filled. To combat social engineering threats effectively, organizations must foster a security-conscious culture, regularly update training programs, and conduct routine security assessments. Implementing a zero-trust security model, enforcing strict access controls, and promoting collaboration in cybersecurity intelligence sharing will further strengthen defense mechanisms. As attackers continue to evolve their tactics, ongoing research and adaptive security frameworks will be crucial in mitigating future threats. By integrating technological innovations with a strong emphasis on user education and organizational policies, this study paves the way for more resilient cybersecurity practices, ultimately reducing the risks associated with social engineering attacks.

[](http://moodle.gatewaycollege.edu.au/)

# **Team Contribution Summary and Verification**

**Member Name & Student ID: Naila Andalive 202211141  
Role and tasks verification:**

1. Detecting what SE attack is and the background of the project.
2. Setting up the goal of the project.
3. Data analysis of the collected survey questions
4. Work distribution among the group and managing timeline.

**Member Name & Student ID: Rojina Lama Syangtan 202211017  
Role and tasks Verifications:**

1. Building up the hypothesis of this project.
2. Recommendation about SE attack prevention
3. Discussed scope of the project.
4. Identified risk and evaluation of the SE attacks

**Member Name & Student ID: Shova Bhujel 202210985  
Role and tasks verifications:**

1. Literature review
2. Detecting problem statement
3. Implementing methodology
4. Extracting the limitation of the project.

**Member Name & Student ID: Bandana Lamichhane 202211167  
Role and tasks verifications:**

1. Identify the gaps of the research
2. Identify the findings of this project.
3. Giving the problem statement for the project.
4. Finding out the key findings of data analysis

# **11 References**

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE), 4*(1), 1-20.

Burda, P., Allodi, L., & Zannone, N. (2024). Cognition in social engineering empirical research: A systematic literature review. *ACM Transactions on Computer-Human Interaction, 31*(2), 1-55.

Gururaj, H. L., Janhavi, V., & Ambika, V. (Eds.). (2024). *Social engineering in cybersecurity: Threats and defenses*. CRC Press.

Samad, A. (2024). Social Engineering in Cybersecurity: Prevention and Mitigation Strategies.

Zaoui, M., Yousra, B., Yassine, S., Yassine, M., & Karim, O. (2024). A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Towards Effective Mitigation Strategies. *IEEE Access*.

Pandey, S., & Chaudhary, A. (2023). Vulnerability scanning. *Authorea Preprints*.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Griffiths, A. (2023). SWRK 540: Social Work Research Methods 3 credit hours Fall 2023 Professor: Dr. Austin Griffiths.

Schneier, B. (2023). *A hacker's mind: how the powerful bend society's rules, and how to bend them back*. WW Norton & Company.

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

Heartfield, R., Loukas, G. and Gan, D., 2016. You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access*, *4*, pp.6910-6928.

Fuertes, W., Arévalo, D., Castro, J. D., Ron, M., Estrada, C. A., Andrade, R., Pena, F. F., & Benavides, E. (2022). Impact of social engineering attacks: A literature review. Developments and Advances in Defense and Security: Proceedings of MICRADS 2021, 25-35.

Ibrahim, U.M.A.R.U., 2019. The Impact of Cybercrime on the Nigerian Economy and banking system. *NDIC Quarterly*, *34*(12), pp.1-20.

Keepnet Labs, 2018. *Breach Level Index: 2018 First Half Review*. [online] Available at: [https://keepnetlabs.com](https://keepnetlabs.com/) [Accessed 23 September 2024

Hadnagy, C., 2018. *Social Engineering: The Science of Human Hacking*. John Wiley & Sons.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E., 2015. Social engineering attacks on the knowledge worker. *Proceedings of the 6th International Conference on Security of Information and Networks*, pp.19-25.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E., 2010. Anti-phishing education: a usability study. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp.373-382.

Tischer, M., Fahl, S., Smith, M. and Schneider, M., 2016. *The state of the art in phishing protection*. Institute of Electrical and Electronics Engineers.

Wang, D., Wang, P., Xu, S. and Sun, J., 2019. *A survey of defense mechanisms against social engineering attacks*. Elsevier.

# **11 Appendix**

## **Appendix A: Objectives**

A diagram of a diagram

AI-generated content may be incorrect.

## **Appendix B: Limitations**



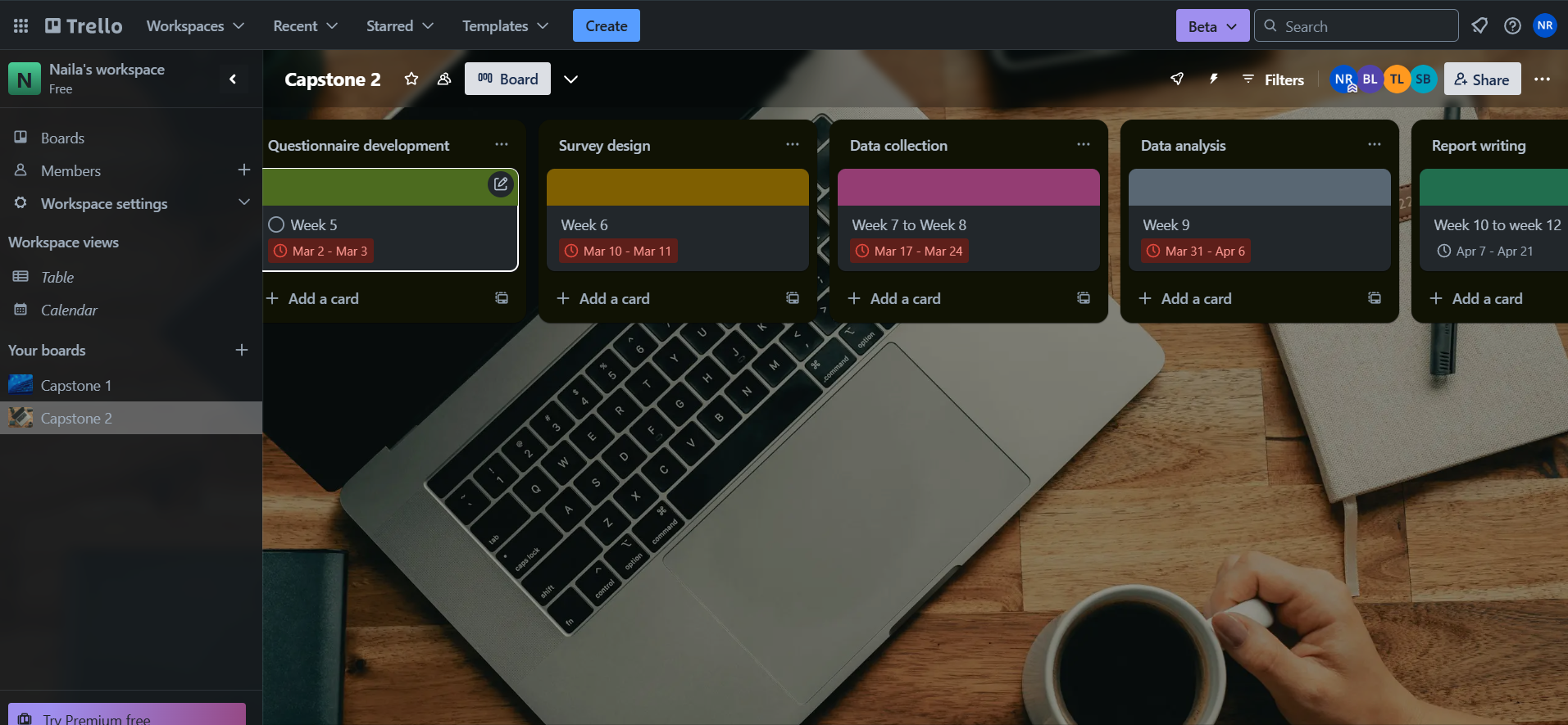
## **Appendix C: Project Plan**

A graph with red squares and numbers

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



## **Appendix I: Survey Questions Screenshot**

A white background with black text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A white screen with black text

AI-generated content may be incorrect.

A white background with black text

AI-generated content may be incorrect.