Mitigating Social Engineering Risks: An Integrated Framework Concurrently Addressing Human Vulnerabilities and Technical Defences in Cybersecurity

MSc Research Project
MSc Cybersecurity

Oreoluwa Emmanuel Ibitowa
Student ID: X23195240

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Oreoluwa Emmanuel Ibitowa

Student ID: X23195240

Programme: MSc Cybersecurity **Year:** 2024/2025

Module: Practicum

Supervisor: Joel Aleburu

Submission Due Date: 12/12/24

Project Title: Mitigating Social Engineering Risks: An Integrated Framework Concurrently Addressing Human Vulnerabilities and Technical Defences in Cybersecurity

Word Count: …………………………………… **Page Count**…………………………………………………..

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: Oreoluwa Emmanuel Ibitowa

Date: ……………………………………………………………………………………………

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):	

Mitigating Social Engineering Risks: An Integrated Framework Concurrently Addressing Human Vulnerabilities and Technical Defences in Cybersecurity

Oreoluwa Emmanuel Ibitowa
X23195240

Abstract

Cyber security continues to be a key concern with growing use of social engineering techniques such as phishing, pretexting, baiting, and tailgating, exploiting psychological triggers such as trust, urgency, and fear, to attack humans. In an attempt to address both technical and human defences, this work introduces an integrated model for social engineering countermeasures. Analysing 154 real-life cases through qualitative analysis, the work identifies repeat attack patterns, psychological exploit mechanisms, and sector-specific vulnerabilities. Drawing a dataset from industry reports, academic studies, and case studies, the work underlines the importance of integration between technology and humans in countering social engineering threats. Composed of three principal pillars, namely, simulation training and awareness programs, multi-factor authentication and behaviour anomaly, and an organizational environment focused on cybersecurity awareness and governance, the proposed model aims to counter social engineering attacks through a balanced integration of humans and technology. Findings reveal that technology alone cannot suffice and must be supplemented with behaviour-related insights for a strong security stance. Emphasis is placed in the work for an inter-disciplinary model combining psychology, cybersecurity, and organizational behaviour for proactive countering of emerging social engineering attack techniques. AI-powered personalized training, real-time adaptability in security protocols, and larger datasets with emerging threats such as deepfake-related phishing must be researched in future studies.

1 Introduction

Cybersecurity has been at the core of concern for multi-million-dollar companies of different industries, driven by continuous digital transformation across the industries. This is where attackers shifted away from purely technical exploits, targeting instead the exploitation of human behaviour as businesses invest in technical defences such as firewalls, encryption, and multi-factor authentication (Schneier, 2021). Social engineering is the elaborate means whereby cyber crooks discover ways of hoodwinking people into revealing confidential information so as to get round even the most robust technical security controls (Hadnagy, 2014; Mitnick & Simon, 2002). In fact, tactics such as phishing, pretexting, baiting, and tailgating all use very fundamental human emotions, like trust, fear, and urgency, to deceive people into an action that compromises security in organizations (Hovav & D’Arcy, 2012b).

While the dependence on digital platforms is increasing, so is the sophistication in cyber-attacks; therefore, an integrated approach to cybersecurity becomes of prime importance, covering precisely technical vulnerabilities and human factors (Algarni et al., 2017). A project entitled "The Human Factor in Cybersecurity" has placed centre stage the role of human psychology in cybersecurity breaches, focusing on how social engineering takes advantage of human vulnerabilities and what strategies are effective to counter these threats (McCormac et al., 2017).

1.1 Significance of study

It is increasingly recognized that the human factor is the weakest link in cybersecurity defences (Verizon, 2020). While technology is advancing, social engineering attacks still do prevail, and they have been causing irreparable monetary loss and data leakage, which ultimately results in reputation loss. The Verizon Data Breach Investigations Report of 2020 points out that human error plays a significant role in most cybersecurity incidents (Verizon, 2020). This gap needs to be addressed in line with organizations seeking to improve their cybersecurity posture (Krombholz et al., 2015).

This research has a great significance in that it connects the key gap between the technical cyber-security measures and the psychological aspect of human behaviour. The incorporation of concepts on cybersecurity, psychology, and the social sciences will hence enable the project to come up with more comprehensive security strategies that protect humans from their vulnerabilities (S. M. Furnell, 2020; McCormac et al., 2017). These could be a bigger dividend in the form of deep insights into social engineering tactics, improved security training, and the development of robust policies mitigating or nullifying the human factor in cybersecurity breaches.

1.2 Research Question and Objectives

Research Question: What role does social engineering play in compromising cybersecurity, and what strategies can mitigate these risks?

The aims of the study will be to establish how social engineering attacks explore human weaknesses and to provide a theoretical framework incorporating technical and human-centred strategies in mitigating such risks. The specific objectives will be to:

- Create a comprehensive dataset using well-documented case studies and industry reports on social engineering attacks.
- Develop an algorithm in Python to analyse the dataset and identify patterns in human vulnerabilities and social engineering tactics.
- Establish a theoretical framework that integrates technical and human-cantered cybersecurity strategies.

This framework will be based on qualitative analysis, integrating insights into cybersecurity, psychology, and social sciences that will help organizations implement technical solutions and policies that improve human awareness and reduce susceptibility to social engineering attacks.

This report discusses social engineering and human vulnerabilities in cybersecurity, starting with the problem's introduction and the question: human susceptibility regarding cybersecurity. The Literature Review will introduce existing research while indicating knowledge gaps and the need for an interdisciplinary approach. Specification of Research Method describes the qualitative research design utilized for data collection and analysis of social engineering tactics. The Conclusion and Recommendations summarize some of the key findings with practical strategies in place to avoid susceptibility in such an attack.

2 Literature Review

In this view, with increased sophistication of social engineering that takes advantage of human psychology to compromise cybersecurity defences, an integrated approach will be necessary, one that incorporates technical safeguards and strategies to mitigate human vulnerabilities. Considering the dual nature of cybersecurity, a complex technology mixed with human factors, the literature has established that comprehensive frameworks are required for solutions in the dual nature of the challenge, emphasizing human-cantered solutions alongside avant-garde technical controls.

2.1 Human Vulnerabilities and Psychological Exploitation

Estella (2024) shows how attackers manipulate the use of psychological triggers-fear, authority-to hoodwink victims. This paper really underlines the embedding of insights from psychology into cybersecurity practices, such as methods for avoiding cognitive overload, and thus making people less vulnerable to social engineering-type attacks. Although highly enlightening, this narrow focus on specific triggers, like fear, is at the cost of systemic and organizational causes for vulnerability. The wider perspective that might be attained from consideration of environmental and cultural contexts would arguably enhance the usefulness of this approach. The foregoing research therefore underpins the psychological basis for social engineering and amplifies the proposal towards human-centred defences (Estella, 2024).

Tikanmäki and Ruoslahti (2024) address cognitive biases exploited by attackers, such as heuristic decision-making that leads to errors under stress. They advocate for embedding educational strategies into technical solutions in order to enhance human decision-making. While theoretically sound, the study lacks empirical validation of its recommendations, especially across diverse cultural and organizational environments. It also points out the need to address cognitive limitations within the broader organizational defences (Tikanmäki & Ruoslahti, 2024).

Social engineering remains a major technique that cybercriminals use to compromise security systems by manipulating basic human feelings and cognitive biases. According to Nobles and Robinson (2024), human factors remain the leading causes of security vulnerability. In this work, the two researchers have pinpointed that even with advanced technology, attackers still manipulate effective psychological triggers such as fear, trust, and authority, enabling them to bypass some of the most sophisticated technical controls. The authors call for the integration of human factors engineering in cybersecurity best practices to reduce such risks through designing user interfaces that have minimum cognitive loads, hence minimizing such users' possibility of causing an error (Nobles & Robinson, 2024).

Similarly, Hasan et al. (2024) analyse how the tendency towards social engineering is susceptible because of the cognitive biases of the targeted individual. They emphasize that attackers leverage heuristic decision-making processes, which manifold are tainted by emotional or incomplete information influences. Their conclusions suggest that cybersecurity strategies cannot rely solely on technical controls but must be complemented with robust user education and awareness. Such initiatives must be directed at addressing common biases in users and arming them with critical thinking skills to recognize and ward off social engineering tactics (Hasan et al., 2024).

2.2 Simulation-Based Learning and Human-Centric Training

Mersni et al. (2024) provide great evidence for simulation-based training in improving real-time response against social engineering tactics. Their results show that immersive, scenario-based exercises significantly improve the phishing detection rate. While the approach is novel, scalability or resource-related issues to conduct such training programs in organizations of different sizes are not considered. Future research could integrate automation tools in a cost-effective way. This work would thus inform the inclusion of scenario-driven modules in the proposed framework because such modules have proven efficient in building cybersecurity awareness (Mersni et al., 2024).

Hovav and D’Arcy (2012) argue that continuous awareness training mitigates social engineering risks by reinforcing security behaviours. Their longitudinal study demonstrates sustained behavioural improvements through regular reinforcement of protocols. Although robust in scope, the study does not explore the dynamic evolution of social engineering threats, necessitating adaptive training approaches tailored to emerging challenges. This work underscores the importance of periodic reinforcement, integral to the project's focus on sustainable human-centric interventions (Hovav & D’Arcy, 2012a).

2.3 Techniques of Social Engineering and Psychological Mechanisms

Sharma et al. (2024) classify different social engineering methods, with its psychological underpinning of phishing, pretexting, and baiting in detail and stress the use of psychometric insights to develop pre-emptive defence strategies. While such different classifications were well thought of, their empirical evidence, to prove such defence strategy, is lacking and not shown in real scenarios. It should be strong if some data-driven validation could integrate to make the practical implications stronger of a study. As a conceptual basis, this sets into the context of coding and analysis of social engineering tactics (Sharma & Varalakshmi, 2024).

Saleem et al. (2024) explore emotional manipulation as a key vulnerability in social engineering, advocating for training programs designed to enhance emotional regulation. They suggest that emotionally resilient individuals are less likely to fall victim to manipulative tactics. Although novel, the study's proposed interventions lack concrete implementation guidelines, making widespread adoption challenging. Emotional resilience training aligns with the project's goals of mitigating psychological vulnerabilities (M. Saleem et al., 2024).

For instance, in 2024, Rupra's outlined in detail various techniques of social engineering: phishing, pretexting, baiting, and tailgating. Identifying them, the research outlines that everything among those has their roots in psychological manipulation, depending upon the attacker's capability to develop a time factor or an authority factor. An attacker forces individuals to perform certain actions without the latter reflecting enough, thus bypassing the rational decision-making processes. In turn, Rupra recommends the development of security frameworks supported by research in psychology to better understand these manipulative tactics and take countermeasures. For example, policies can aim at introducing delays into immediate responses to security-critical communication that allows users a chance to consider if their requests are legitimate (Rupra, 2024).

2.4 The Evolution of Social Engineering in the Digital Age

Petropoulou and Varouchas (2024) look at how technological development, in particular social media, has tailored social engineering attacks. Much of the focus in their work is on adaptive training programs, which change as the threat landscape changes. This research makes a valuable contribution but falls short regarding insider threats, considered crucial in developing effective defences. If this limitation were addressed in its scope, it would prove even more useful. The study cements the dynamic nature of social engineering, hence the need within the framework for continuous monitoring and training (Petropoulou & Varouchas, 2024).

Hutchins et al. (2024) extend the Cyber Kill Chain framework to include social engineering-specific tactics, emphasizing the disruption of attackers' workflows through targeted interventions. While comprehensive, the model underrepresents human vulnerabilities, limiting its application in addressing non-technical aspects of security. This work provides structural insights into integrating human-centred strategies within technical frameworks (Hutchins & others, 2024).

2.5 Integrating Technical and Human-Cantered Security Frameworks

It is in this respect that the literature also discusses the development of integrated security frameworks incorporating both technical and human-side factors. Nifakos et al. (2024) propose a multilayered cybersecurity framework that embeds behavioural analytics with machine learning algorithms to adapt to evolving threats. Their approach integrates human factors with technical defences for holistic security. While the framework is robust, its reliance on advanced technologies may make it too expensive for smaller organizations. Simplifications for more general applicability should be explored. The study shows the potential of combining human and technical approaches as reflected in the framework of the project (Nifakos et al., 2024).

Furnell (2020) definitely stresses the shortcomings of reactive measures and insists on the necessity of more proactive strategies, like predictive modelling and behavioural analytics, which would serve to keep one step ahead of the attackers. It would be even better if this research underlined an organizational culture as a factor that promotes cybersecurity readiness. This should be included as yet another dimension. This research has supported the focus being placed by the current project on proactive and anticipatory defences (S. Furnell, 2020).

Therefore, Saleem et al. (2024) define a multilayered framework in machine learning algorithms, threat detection, behavioural analytics, insider risk, and phishing attempts. The integrated framework makes use of information extracted from the data-driven insights for prediction and mitigation of potential threats while inculcating human behavioural analysis for pre-emptive addressing of vulnerabilities. Saleem affirm that such frameworks have to be adaptive, continuously changing in respect of newly emerging threats with regard to new knowledge about human behaviour (A. Saleem et al., 2024).

Schneier (2021) further stresses the limitations of reactive security measures only. His studies call for proactive strategies that incorporate threat intelligence, user behaviour analytics, and predictive modelling. Using advanced analytics and machine-learning techniques, an organization can identify unusual patterns indicative of a social engineering attack. He calls for a change in tack toward anticipatory defence mechanisms whereby the organization might not just respond to breaches but forecast them and forestall such incidents by continuous monitoring and learning (Schneier, 2021).

2.6 Framework for Holistic Cybersecurity

Drawing on those lessons, Sadaat (2024) goes further to provide an integrated framework that considers both the technical and human vulnerabilities. This framework insists on proactive, culture-driven cybersecurity in which awareness and vigilance are integrated into every facet of organizational operations. In this respect, Sadaat points out that organizations should invest in the development of behavioural analytics, user-friendly security technologies, and continuous education (Sadaat, 2024). Some of the measures it would include in the proposed framework are: design of interfaces to reduce the chances of error and simplify security-critical tasks, use of analytics for detecting variance from normal behaviour that may signal an account compromise, regular simulation-based training in order to prepare employees for evolving social engineering tactics, and fostering an environment of cybersecurity as a shared responsibility and it being comfortable for employees to report suspicious activities.

The literature recognizes this need for a holistic and integrated cybersecurity approach. Since it attacks the human psychology, given that socially engineered attacks are effective in most past instances, such vulnerabilities need to be addressed through technical innovation coupled with human-cantered strategies. It is only when advanced threat detection systems are knitted together with comprehensive user education and further integrated with behavioural analytics that resilient security frameworks may emerge at organizations. The study confirms the idea that just an interdisciplinary proactive approach will be able to reduce the factors of vulnerability to social engineering and enhance general cybersecurity.

3 Research Methodology

The paper employs an overall qualitative methodology to investigate the role of social engineering in cybersecurity breaches, focusing on how human factors drive organizational vulnerability. This research design encompasses the following stages: research design, data collection, sample preparation, data analysis, framework development, and findings validation. Each of these was designed to rigorously analyse the impact of social engineering on cybersecurity using a multidisciplinary approach that integrates knowledge from psychology, cybersecurity, and the social sciences (Hasan et al., 2024; Nobles & Robinson, 2024).

3.1 Research Design

This study adopts an exploratory and qualitative research design to investigate the ways in which human psychology and behaviour impact cybersecurity vulnerabilities. Given the complex, human-centric nature of social engineering attacks, qualitative methods were chosen to allow for a deeper understanding of the subtle psychological mechanisms that attackers exploit. This approach facilitates the exploration of human behavioural aspects that quantitative data alone may not reveal, such as cognitive biases, emotional triggers, and decision-making under pressure (Alsulami, 2024; Mersni et al., 2024).

3.2 Data Collection

3.2.1 Data Sources

The data is based on a wide outlook from secondary sources, such as case studies and industry reports. Actual incidents of social engineering attacks were identified through cybersecurity reports, company disclosures, and news articles. Some of the well-documented cases here include the Colonial Pipeline ransomware attack in 2021, partially caused by social engineering. Data on social engineering trends, tactics, and consequences was extracted from annual reports such as the Verizon Data Breach Investigations Report, 2024, and reports by cybersecurity firms such as CrowdStrike and CyberArk (Crowdstrike, 2024; Cyberark, 2024; Verizon, 2020).

3.2.2 Collection Techniques

In the case of industry reports and case studies, document analysis methods were utilized to extract relevant data on the types of social engineering tactics used, psychological triggers exploited, and impacts on organizations. Qualitative coding was used to identify recurring themes and patterns in social engineering tactics and mitigation measures (Hasan et al., 2024; Mersni et al., 2024).

3.3 Sample Selection and Preparation

To ensure that the research covers a wide range of social engineering tactics and impacts, cases were selected based on the following: incidents that resulted in huge losses or disruption of operations were selected to show the severity of social engineering threats; cases that represent various techniques of social engineering-for example, phishing, baiting, pretexting-were selected to give a broad perspective on the different tactics used by attackers. This is followed by the cleaning of data, whereby irrelevant information is removed and inconsistencies are normalized. For example, excess technical details not directly relevant to human factors were removed. The data were then transformed into structured categories of format: which tactic used, which psychological trigger is exploited, organizational impact, and response strategy.

3.4 Analytical technique

The data analysis comprised of a few steps to ensure a thorough examination of human vulnerabilities in cybersecurity:

- Qualitative Coding: Using Python, qualitative coding was employed to identify and categorize key themes related to psychological triggers (e.g., trust, fear, authority), social engineering techniques, and organizational impacts.
- Comparative Case Analysis: A comparative analysis was conducted across different case studies to uncover common tactics, recurring psychological triggers, and patterns in organizational responses. This allowed for the identification of gaps in current cybersecurity practices and the consistency of social engineering's psychological impact across various settings (Alsulami, 2024; Rehan & Patterson, 2024).

4 Design Specification

The social engineering attack design specification details an integrated approach to understanding the issue at hand and mitigating risks caused both at the level of technical vulnerability and the so-called human factor. Integrated research methodology, using qualitative analysis, will be put in place. Underpinning architecture integrates human-centred insights from psychology and behavioural sciences into advanced cybersecurity technologies.

4.1 Design process

These will be supplemented with a number of case studies, well-documented from known cyber-incident reports, which shed light on how social engineering attacks have been carried out or mitigated. Data thematic analysis and qualitative coding shall attempt to identify patterns in tactics associated with social engineering and vulnerable humans. Key themes will be identified and analysed for informing the framework. This will, therefore, be developed into a theoretical framework for the project that incorporates technical defences with human-centred strategies in a holistic approach to strengthening organizational cybersecurity (Mersni et al., 2024; Nobles & Robinson, 2024).

4.2 Flow chart

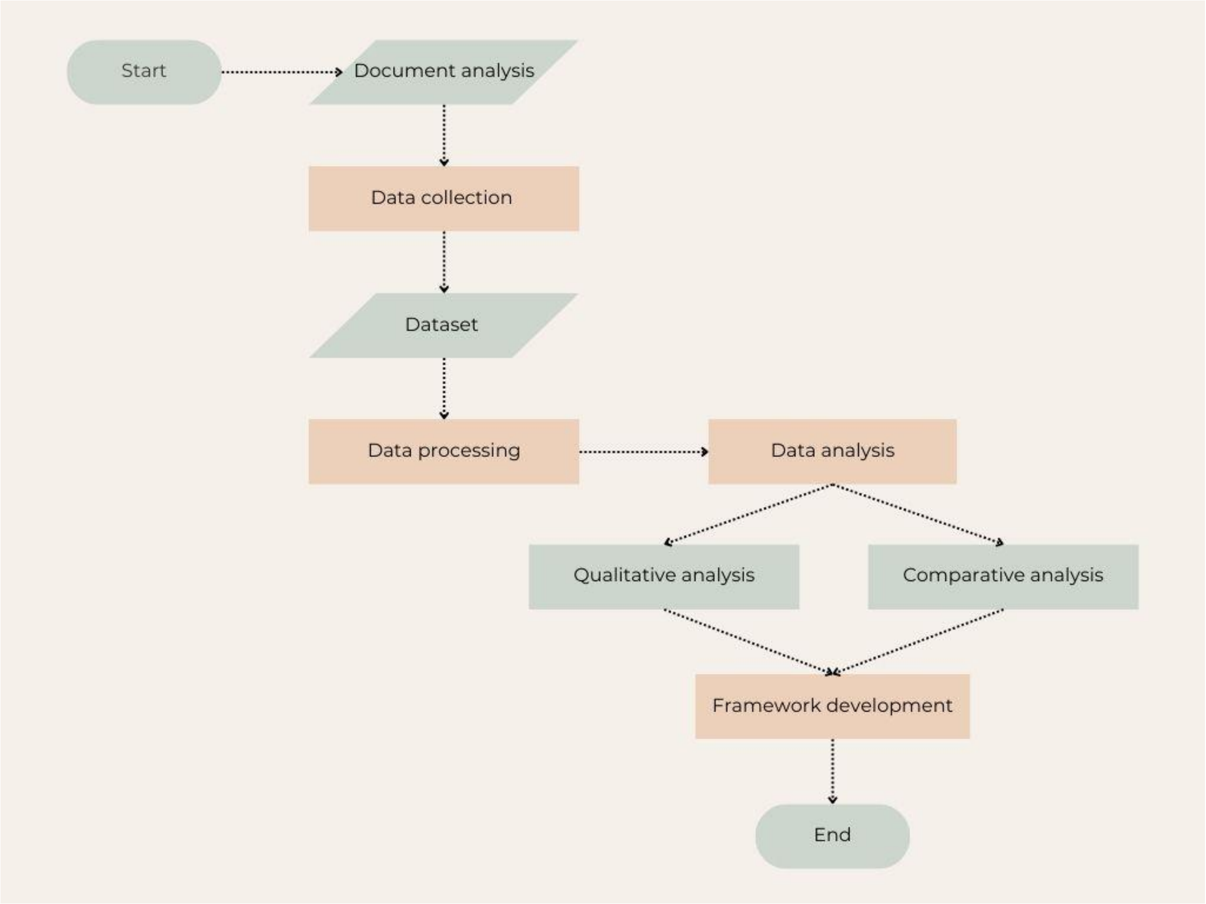


Figure 1: Flowchart

4.3 Implementation and Outputs

Implementation of the project will involve Python for complete data analysis. This involves the implementation of Pandas to organize and structure a dataset on user behaviour patterns, while numpy will be used in the context of deep qualitative analysis. Likewise, the comparison analysis of narrative data from case studies using the library numpyy will allow a very detailed investigation of the patterns and trends within qualitative insights. Besides, a comprehensive review of heavy documentation would be included, such as an industrial report, case study, and academic literature to review some of the critical studies into current findings on social engineering tactics via identifying key themes, as well as useful insights. Key proposed outputs necessary to complete this project were to provide an advanced dataset related to user behaviour patterns, which would indicate best practices, integrated with a cybersecurity framework in which findings would be applied, thus helping reduce risk from social engineering.

5 Implementation

This implementation phase of the project tried to translate the research methodology into concrete and actionable steps needed to derive desired outcomes. These three key deliverables entailed a strong dataset, qualitative insights, and a theoretical cybersecurity framework. Their alignment with the greater streams of objectives will also be helpful in understanding and mitigating the risks of social engineering, both technical and human vulnerabilities.

The major output was the development of an extended dataset, including 154 unique cases of social engineering attacks. Much care was taken to create this dataset, reproducible in the future for qualitative analysis. Each entry had comprehensive attributes like incident descriptions, types of attacks, psychological triggers exploited, organizational impacts, and the preventive measures adopted. The diverse and comprehensive structure of this dataset offers far-reaching qualitative analysis and forms a useful basis for future research in this area. For instance, data from incidents like the Colonial Pipeline ransomware attack (Robinson, 2024), complemented by industry reports from sources such as CrowdStrike 2024 (Crowdstrike, 2024), CyberArk 2024 (Cyberark, 2024), and Verizon's Data Breach Investigations Report 2024 (Verizon, 2024), ensured the dataset's comprehensiveness and relevance.

The second output was qualitative insights derived from the dataset. The recurring patterns of human vulnerabilities and the psychological mechanisms that were exploited in social engineering attacks came out in the analysis. These insights showed common attack types, such as phishing and baiting, with their psychological triggers like fear, trust, and urgency that attackers frequently manipulate. The analysis has also demonstrated that these kinds of attacks have deep organizational implications and how necessary comprehensive defences in both human and technical dimensions are.

The third deliverable was a theoretical framework of cybersecurity synthesizing technical and human-centred strategies for mitigating social engineering risks. These are proposed recommendations that take the form of actionable advanced training programs for staff, technical security controls incorporating multi-factor authentication, and organizational policies that foster improved cybersecurity awareness and resilience. These strategies will be informed by best practices, along with qualitative insights, which balance the need for technical robustness with human behavioural interventions.

The project required advanced tools and methodologies during its implementation. Python was the major programming language used throughout the collection and preprocessing of data and its analysis, where key libraries included pandas for data manipulation/structuring (McKinney, 2010), numpy for natural language processing and text analysis (S. Bird E. Klein & Loper, 2009), and matplotlib for visualizing data trends (Hunter, 2007). The information sources included academic research, case studies, and industrial reports. Incident descriptions were standardized and analysed in concert with the overall project objectives. Once finalized, the dataset was exported in.csv format as per the requirement for ease of access and compatibility with various platforms of analytical tools.

The implementation followed a structured series of steps in order to ensure rigor and precision in the methodology. First, data collection was carried out by identifying reliable sources such as case studies and industry reports. This phase focused on extracting comprehensive incident descriptions, including attack type, psychological triggers, and impacts. Data cleaning ensured consistency and removed duplicate or irrelevant entries, thus maintaining dataset integrity. The next step after data cleaning was the development of a standardized dataset with entries that would stand up to scrutiny. This was followed by quantitative analysis, for which Python and other qualitative tools were used for the coding of recurring themes, which included the exploitation of trust and manipulation of authority. Such comparative case analyses across sectors and attack types furthered insight into the trends and vulnerabilities. The insights provided by the qualitative analysis were integrated with the proposed cybersecurity framework, which provides actionable strategies, both technical and related to human factors.

6 Evaluation

The analysis of **154 social engineering cases** provides critical insights into the interplay of psychological manipulation, technical vulnerabilities, and organizational resilience. The results not only illuminate recurring patterns and vulnerabilities but also highlight the significance of interdisciplinary strategies for mitigating these risks. Below, the results are categorized to address the research objectives, ensuring a robust narrative backed by data and analysis.

6.1 Prevalence of Social Engineering Tactics

The dataset highlights the prominence of various social engineering methods in figure 2:

- **Phishing:** Accounting for most of the attacks seen in figure 2, phishing remains the most widespread tactic. Variants include email phishing, spear phishing, and smishing, each exploiting urgency or fear to deceive victims. For instance, attackers often impersonated financial institutions, requesting immediate action to "secure accounts."
- **Baiting:** baiting involved scenarios where attackers offered free resources, such as USB drives or downloads, laced with malware.
- **Pretexting:** this tactic relied heavily on building a rapport through fabricated identities or scenarios, targeting high-level executives in many cases.
- Tailgating and other niche methods, often requiring physical proximity to the target organization.

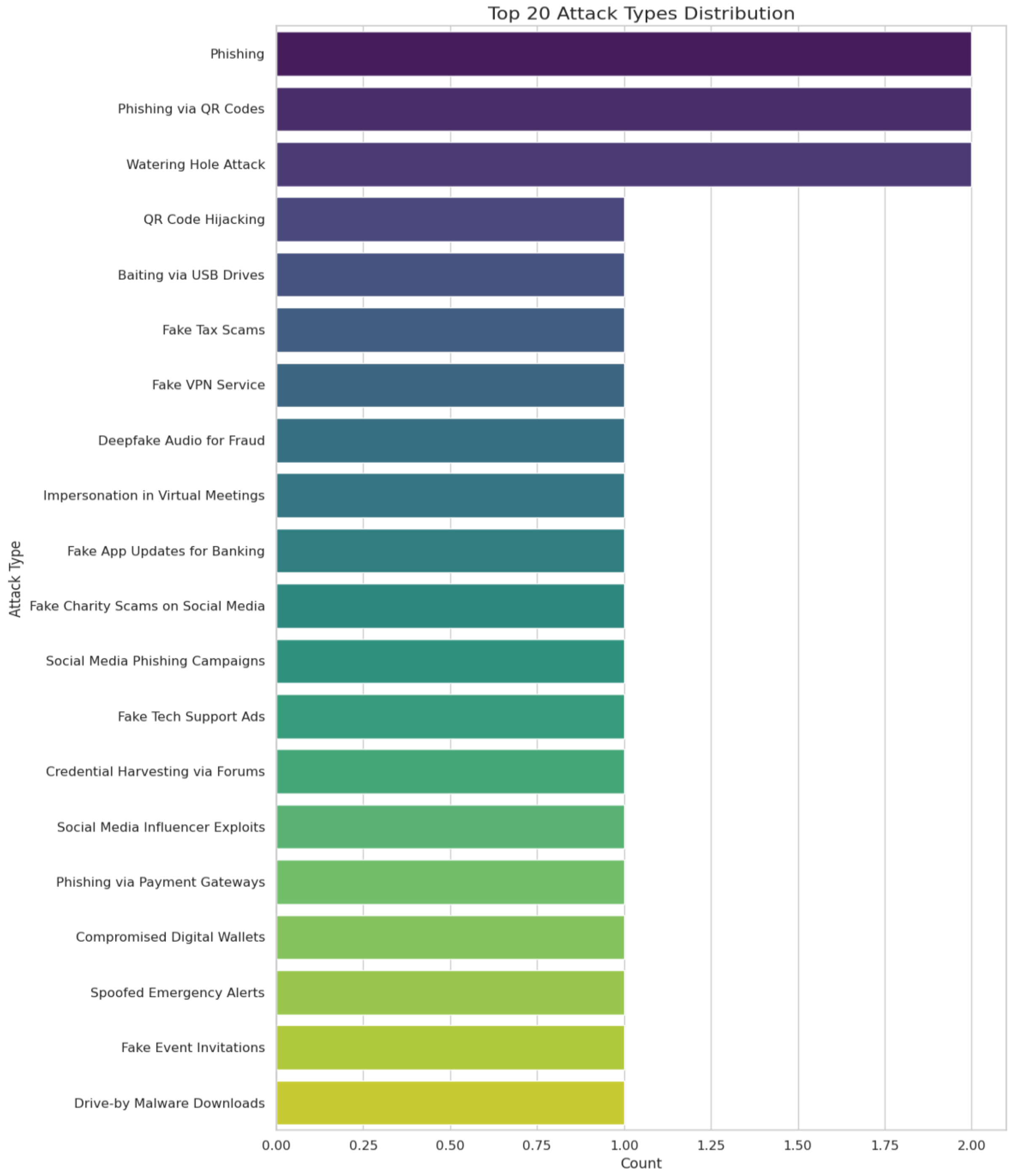


Figure 2: Top 20 Attack Types

6.2 Psychological Triggers Exploited by Attackers

The psychological aspect of social engineering emerged as a significant factor:

- Trust: Found in nearly half of the cases shown in figure 3, attackers impersonated known entities or colleagues to gain credibility. For example, pretexting attacks frequently exploited this trigger by mimicking CEOs or IT personnel.
- Curiosity: Having the second hight number seen in figure 3, these triggers caused victims to want to know more without verifying the legitimacy of requests. Examples include warnings of account suspension or imminent deadlines for action.

- Authority Exploitation: Attackers invoked hierarchical power to coerce action, such as wire transfers or granting system access.

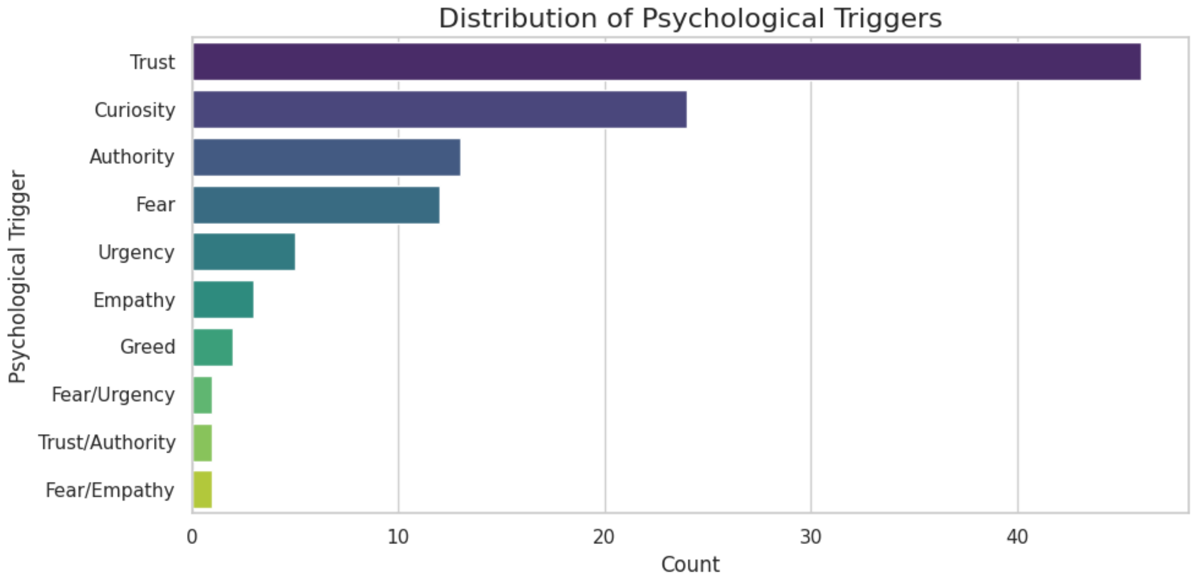


Figure 3: Distribution of Psychological Triggers.

6.3 Attack Impacts

The repercussions of social engineering attacks were multi-faceted:

- Financial Losses: Topping the chart shown in figure 4, with retailers and finance sectors reporting the highest impacts due to sensitive data breaches.
- Reputational Damage: second on the chart seen in figure 4, reputational damage, organizations experienced decline in customer trust, often reflected in attrition rates and diminished market value.
- Operational Disruption: Coming third on the chart in figure 4, with ransomware attacks initiated via phishing emails causing delays ranging from hours to weeks. With figure 5 showing this reflects

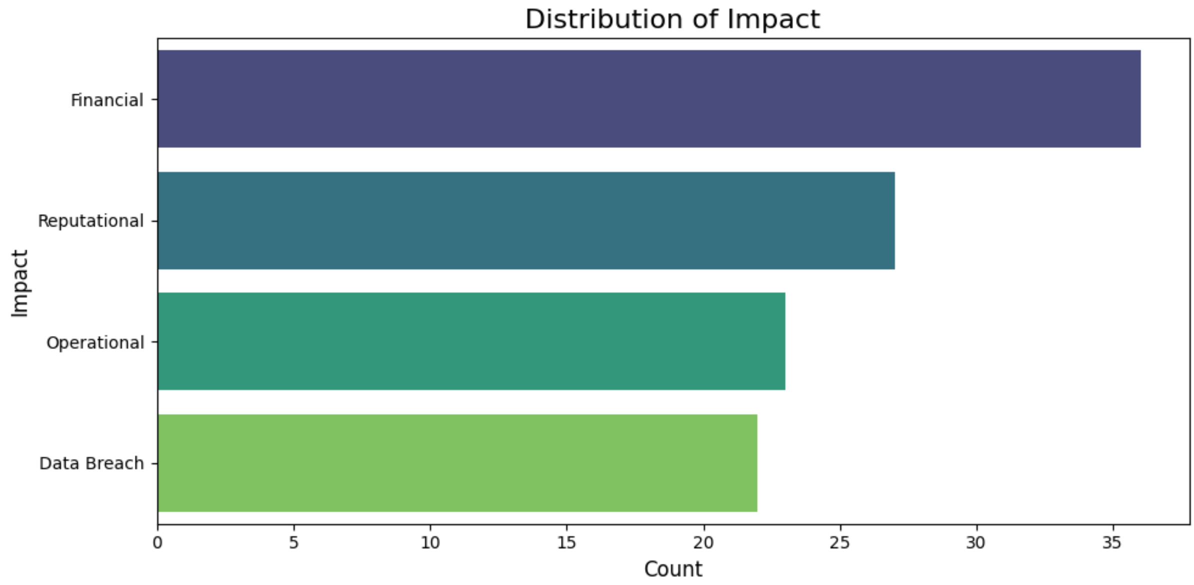


Figure 4: Distribution of Impact

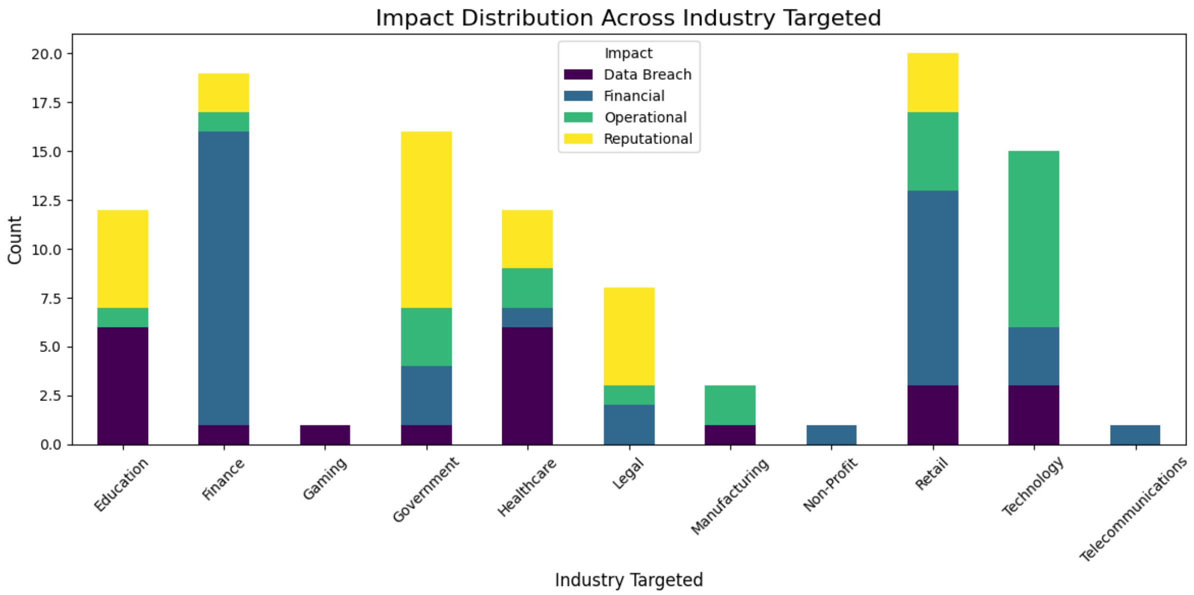


Figure 5: Impact Distribution Across Industry targeted.

6.4 Industry Sector Vulnerabilities

The dataset revealed sector-specific vulnerabilities:

- **Retail:** Representing majority of the targeted industries shown in figure 6, attackers leveraged baiting tactics, such as fake discount offers or gift cards, to compromise customer accounts.
- **Finance:** Second on the chart in figure 6, high-value financial transactions and customer data were frequently exploited, often through phishing and pretexting.
- **Technology:** Third on the chart in figure 6.
- **Healthcare:** Fourth on the list in figure 6 this sector's reliance on legacy systems and sensitive patient data made it a prime target.

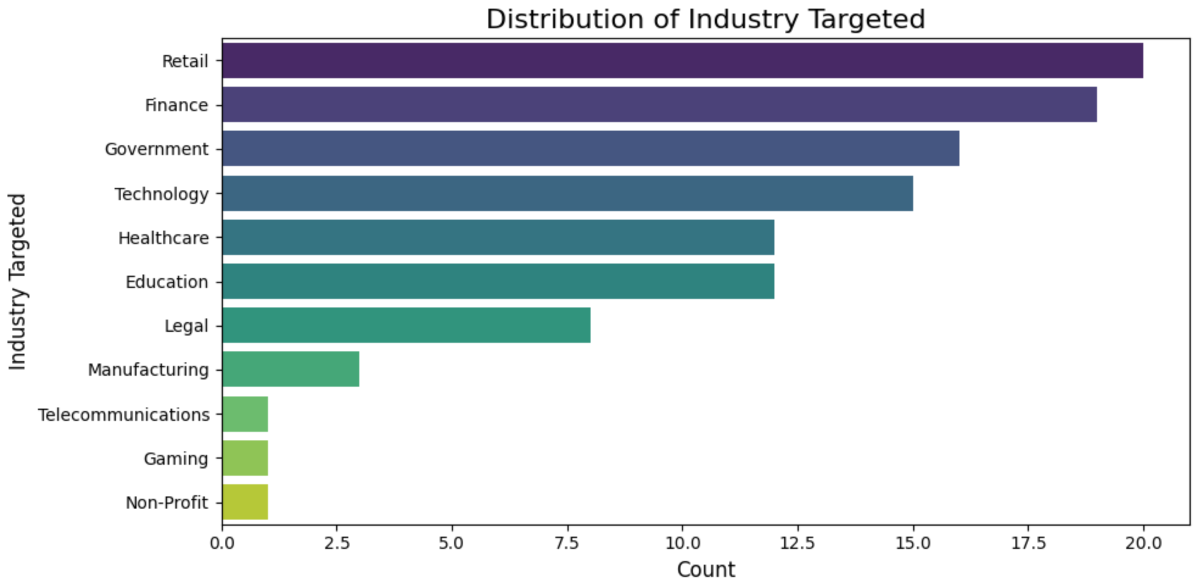
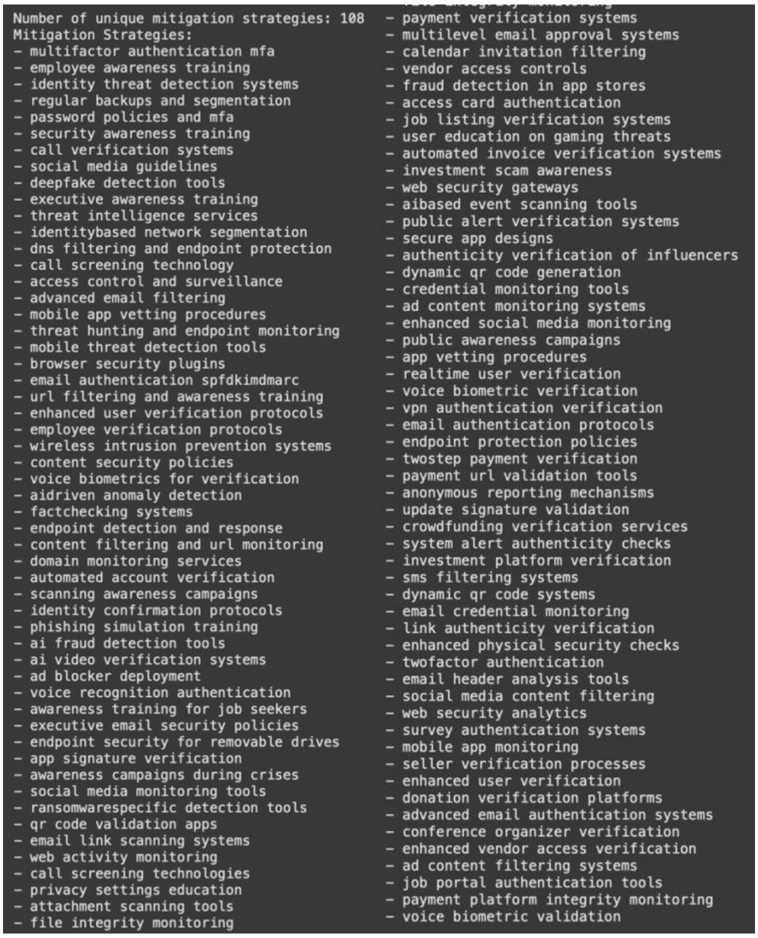


Figure 6: Distribution of Industry Targeted.

6.5 Industry Mitigation Strategy

Comparative analysis highlighted varying levels of resilience among industries employing different strategies to mitigate different attacks seen in figure 8 and the qualitative analysis identified 108 unique mitigation strategies as shown in figure 7:



```
Number of unique mitigation strategies: 108
Mitigation Strategies:
- multifactor authentication mfa
- employee awareness training
- identity threat detection systems
- regular backups and segmentation
- password policies and mfa
- security awareness training
- call verification systems
- social media guidelines
- deepfake detection tools
- executive awareness training
- threat intelligence services
- identitybased network segmentation
- dns filtering and endpoint protection
- call screening technology
- access control and surveillance
- advanced email filtering
- mobile app vetting procedures
- threat hunting and endpoint monitoring
- mobile threat detection tools
- browser security plugins
- email authentication spfdkimdmarc
- url filtering and awareness training
- enhanced user verification protocols
- employee verification protocols
- wireless intrusion prevention systems
- content security policies
- voice biometrics for verification
- aidriven anomaly detection
- factchecking systems
- endpoint detection and response
- content filtering and url monitoring
- domain monitoring services
- automated account verification
- scanning awareness campaigns
- identity confirmation protocols
- phishing simulation training
- ai fraud detection tools
- ai video verification systems
- ad blocker deployment
- voice recognition authentication
- awareness training for job seekers
- executive email security policies
- endpoint security for removable drives
- app signature verification
- awareness campaigns during crises
- social media monitoring tools
- ransomwarespecific detection tools
- qr code validation apps
- email link scanning systems
- web activity monitoring
- call screening technologies
- privacy settings education
- attachment scanning tools
- file integrity monitoring
- payment verification systems
- multilevel email approval systems
- calendar invitation filtering
- vendor access controls
- fraud detection in app stores
- access card authentication
- job listing verification systems
- user education on gaming threats
- automated invoice verification systems
- investment scam awareness
- web security gateways
- aibased event scanning tools
- public alert verification systems
- secure app designs
- authenticity verification of influencers
- dynamic qr code generation
- credential monitoring tools
- ad content monitoring systems
- enhanced social media monitoring
- public awareness campaigns
- app vetting procedures
- realtime user verification
- voice biometric verification
- vpn authentication verification
- email authentication protocols
- endpoint protection policies
- twostep payment verification
- payment url validation tools
- anonymous reporting mechanisms
- update signature validation
- crowdfunding verification services
- system alert authenticity checks
- investment platform verification
- sms filtering systems
- dynamic qr code systems
- email credential monitoring
- link authenticity verification
- enhanced physical security checks
- twofactor authentication
- email header analysis tools
- social media content filtering
- web security analytics
- survey authentication systems
- mobile app monitoring
- seller verification processes
- enhanced user verification
- donation verification platforms
- advanced email authentication systems
- conference organizer verification
- enhanced vendor access verification
- ad content filtering systems
- job portal authentication tools
- payment platform integrity monitoring
- voice biometric validation
```

Figure 7: list of unique mitigation strategies.

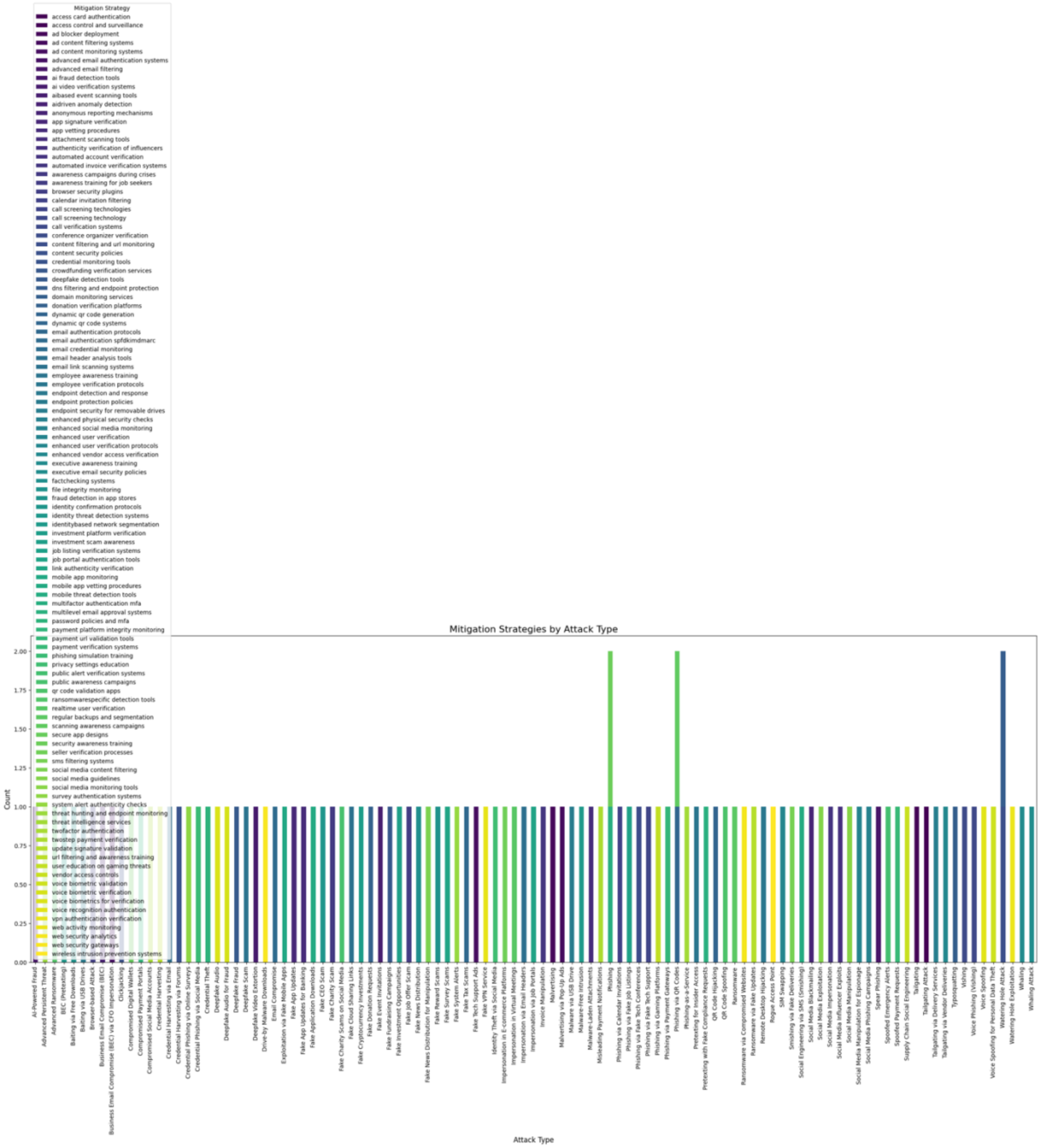


Figure 8: Mitigation Strategies by Attack Type.

6.2 The Theoretical Framework

The framework integrates using information drawn out of the analysis of the dataset to incorporate technical and human-centric approaches to create a resilient organizational defence against social engineering. The framework consists of three interrelated pillars:

- Human-Centric Strategies
- Advanced Technical Controls
- Organizational Culture and Governance

6.2.1 Human-Centric Strategies

Human vulnerabilities form the weakest link in cybersecurity, as highlighted by the dominance of phishing attack having the highest number and the exploitation of psychological triggers like trust, curiosity, authority, fear and urgency as seen in figure 9. To address these, emphasizes needs to be made on the following.

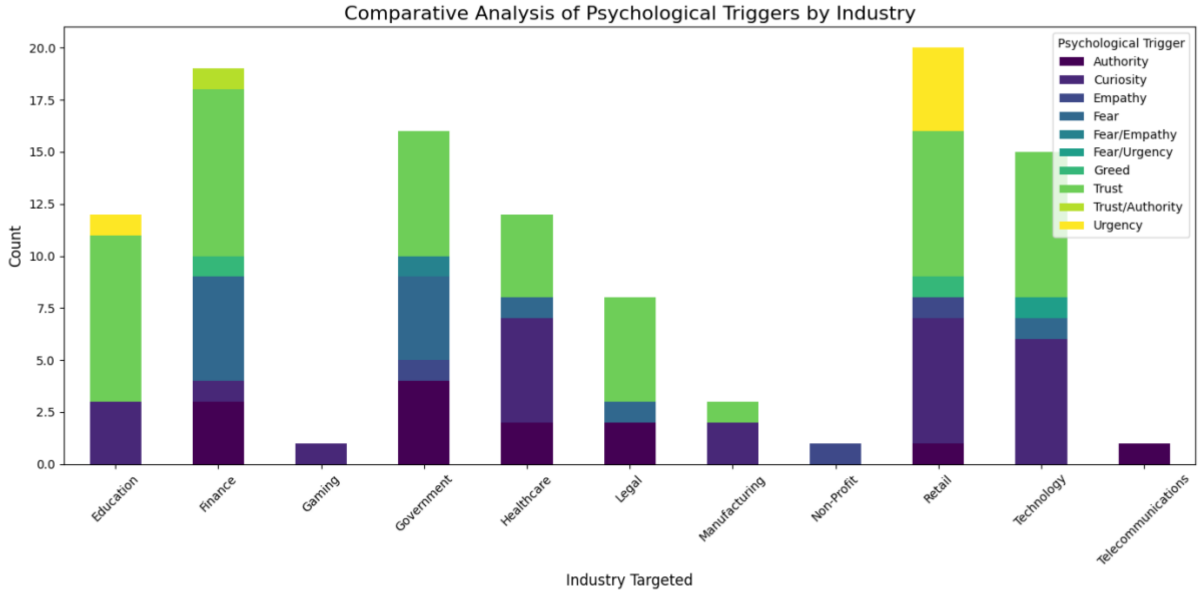


Figure 9: Comparative Analysis of Psychological Triggers by Industry

1. **Simulation-Based Training**

- **Scenario-Driven Exercises**:
  - Real-world phishing simulations specific to industry contexts.
  - Interactive exercises highlighting baiting, pretexting, and tailgating scenarios.
- **Adaptive Modules**:
  - Customizable for organizational roles, e.g., executives (pretexting risks) and IT staff (technical exploitation).

2. **Emotional Resilience Development**

- **Regulation Techniques**:
  - Training to manage cognitive overload, stress, and impulsive decision-making under simulated urgent scenarios.

3. **Awareness Campaigns**

- **Visual and Digital Communication**:
  - Infographics, micro-learning videos, and quizzes tailored to highlight evolving threats.
- **Regular Updates**:

- Threat landscape reports to keep employees informed about emerging attack methods.

6.2.2 Advanced Technical Controls

Social engineering thrives on bypassing standalone technical measures. The dataset and analysis revealed that multi-factor authentication (MFA) is the best mitigation strategy for phishing attacks seen in figure 10.

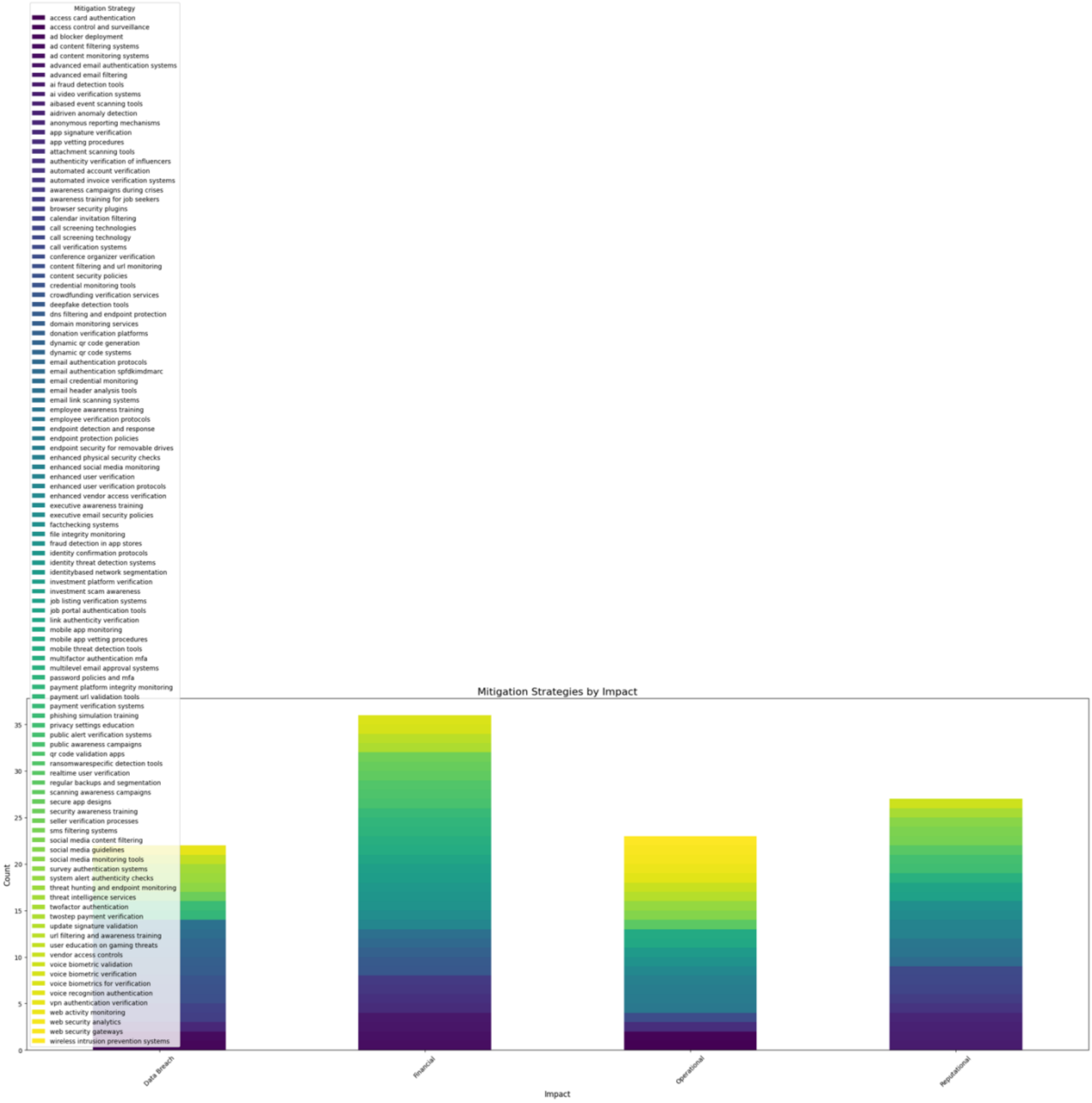


Figure 10: Mitigation Strategies by Impact.

1. **Multi-Factor Authentication (MFA)**

- **Implementation**:
  - Mandatory for all systems handling sensitive data or financial transactions.
- **Context-Aware Security**:

    - Risk-based authentication using geographic and temporal indicators.

2. **Behavioural Analytics and Anomaly Detection**

- **Real-Time Monitoring**:
    - Machine learning models trained on user activity to flag deviations indicative of compromised credentials or malicious insider activity.
- **Predictive Analytics**:
    - Forecasting high-risk periods or user groups based on historical data.

3. **Secure Access Control Protocols**

- **Role-Based Access**:
    - Limiting data access based on job requirements and clearance levels.
- **Time-Limited Permissions**:
    - Expiring credentials for temporary access to minimize risks linked to tailgating.

6.2.3 Organizational Culture and Governance

Cybersecurity is as much a cultural initiative as it is technical. Results showed that organizations fostering a shared responsibility for security are prune to attacks.

1. **Cybersecurity Awareness as a Core Value**

- **Top-Down Leadership**:
    - Executives actively demonstrating security best practices.
- **Cross-Functional Security Teams**:
    - Involving non-IT roles to embed security in daily workflows.

2. **Policy-Driven Protocols**

- **Verification Systems**:
    - Mandatory two-person verification for financial transactions over a threshold.
- **Incident Reporting Channels**:
    - Anonymous mechanisms enabling employees to report suspicious activities without fear of reprisal.

3. **Continuous Improvement**

- **Quarterly Evaluations**:
    - Assessing training effectiveness, technical measure performance, and organizational readiness.

- **Feedback Loops**:
    - Gathering insights from employees to refine interventions.

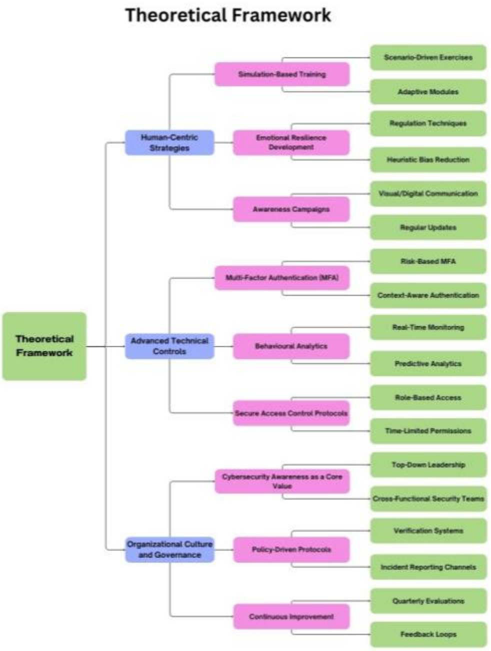


Figure 11: Theoretical Framework

Conclusion and Future work

Social engineering, the use of human weakness to leverage openings even into the most advanced defence mechanisms, remains one of the key cybersecurity threats at present. In the discussion herein, against a background of in-depth integrated analyses of 154 unique incidents, emphasis has been drawn to the duality with which social engineering targets human psychologies as much as technical vulnerabilities. Key findings showed that phishing was the most prominent attack method, which relies on psychological triggers to compromise security, such as trust, curiosity, authority, fear, and urgency. The analysis underlined major financial, reputational, and operational impacts across various industries, with retail and finance being the most hit.

The proposed theoretical framework is holistic in nature, mitigating the risks of social engineering by emphasizing three interrelated pillars:

Human-Centric Strategies: Simulation-based training, emotional resiliency development, continuous awareness on human vulnerabilities.

Advanced Technical Controls: Multifactor authentication, behavioural analytics, and role-based access protocols for strengthening technical defences.

Organizational Culture and Governance: Establish cybersecurity awareness as part of the corporate culture, establish policy-driven protocols, and create a continuous improvement environment. It is a framework that provides a bridge between technical solutions and human-centred strategies or solutions necessary to cope with the change in landscape. The study reveals that mitigating risks of social engineering needs to be proactive and multi-disciplinary, pulling together insights from psychology, cybersecurity, and organizational behaviour in a comprehensive manner.

Future work should concentrate on the enhancement of the proposed framework in three major ways: empirical validation in real-world scenarios across industries regarding effectiveness and long-term impact; advanced AI-driven training modules, tailored to roles and industry-specific threats that improve user preparedness; and enhancement of behavioural analytics through the integration of machine learning for improved anomaly detection and predictive analytics. Expanding the dataset to include diverse cases and emerging tactics, such as deepfake-based phishing, will ensure broader applicability. Grating cultural and regional variations in susceptibility can help with improving strategy customization, while standardized frameworks This will keep the framework adaptive to an ever-evolving threat landscape.

Reference

Algarni, A., Xu, Y., Chan, T.-W., & Tian, Y. (2017). Social engineering in social networking sites: Impact and analysis. *International Journal of Computer and Information Engineering*, *11*, 22–37.

Alsulami, F. (2024). The role of educational interventions and fear appeals in phishing susceptibility reduction. *Cybersecurity Training and Awareness*, *15*, 330–344.

Crowdstrike. (2024). *The 2024 edition of the CrowdStrike Global Threat Report arrives at*.

Cyberark. (2024). *Threat Landscape Report 2024*.

Estella, L. (2024). SOCIAL ENGINEERING: Techniques and Defenses Against Manipulative Attacks. *ResearchGate*. https://www.researchgate.net/publication/385092050

Furnell, S. (2020). Proactive Security Measures in the Digital Age. *Cybersecurity Review*, *4*(2), 127–134.

Furnell, S. M. (2020). Cybersecurity in the Digital World. *Cybersecurity Research and Applications*, *11*, 345–356.

Hadnagy, C. (2014). *Social Engineering: The Art of Human Hacking*. Wiley.

Hasan, I., Zhang, L., & Cohen, M. (2024). Human vulnerabilities in cybersecurity: Exploring cognitive biases in social engineering attacks. *Journal of Cybersecurity Research*, *17*, 102–115.

Hovav, A., & D'Arcy, J. (2012a). Applying Behavior-Based Countermeasures to Cybersecurity Threats. *Computers & Security*, *31*(3), 431–445. https://doi.org/10.1016/j.cose.2012.03.003

Hovav, A., & D'Arcy, J. (2012b). The effect of denial-of-service attack announcements on the market value of firms. *Risk Analysis*, *32*(3), 473–487.

Hunter, J. D. (2007). *Matplotlib: A 2D Graphics Environment*. Computing in Science & Engineering.

Hutchins, E., & others. (2024). Adaptive Cybersecurity Training for the Digital Age. *Springer*. https://link.springer.com/article/10.1007/s11042-024-20059-4

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122.

McCormac, A., Parsons, K., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 369–375.

McKinney, W. (2010). *Data Structures for Statistical Computing in Python*. Proceedings of the 9th Python in Science Conference.

Mersni, A., Yu, W., & Li, J. (2024). Strengthening cybersecurity through simulation-based training and human factors analysis. *Cybersecurity Education Review*, *9*, 250–267.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

Nifakos, S., Chandramouli, K., & Stathakarou, N. (2024). Human Behavior Impact in Cybersecurity. *Springer*. https://link.springer.com/chapter/10.1007/978-3-031-66708-4_8

Nobles, T., & Robinson, M. (2024). Integrating human factors engineering into cybersecurity practices. *Human Factors and Cybersecurity*, *10*, 88–103.

Petropoulou, M., & Varouchas, S. (2024). Social engineering and the influence of social media: New avenues for cybersecurity threats. *Digital Threats and Security*, *13*, 123–138.

Rehan, O., & Patterson, L. (2024). The financial and operational impact of social engineering attacks on organizations. *Journal of Information Security*, *22*, 210–229.

Robinson, P. (2024). *ABOUT THIS CASE STUDY How Lepide Would Have Helped to Prevent the Colonial Pipeline Attack CASE STUDY*.

Rupra, S. (2024). Exploitation of psychological triggers in social engineering: A study on phishing and pretexting. *Social Engineering Studies*, *5*, 76–88.

S. Bird E. Klein, & Loper, E. (2009). *Natural Language Processing with Python*. O'Reilly Media.

Sadaat, F. (2024). Fostering cybersecurity awareness as a proactive measure against human errors in security. *International Journal of Cybersecurity and Privacy*, *8*, 150–167.

Saleem, A., Nguyen, B., & Kumar, S. (2024). Towards a multi-layered cybersecurity framework: Integrating AI and human behavioural insights. *Journal of Cyber Threat Detection*, *19*, 203–221.

Saleem, M., Kumar, R., & Chawla, C. (2024). Understanding the Human Factors in Cybersecurity. *ResearchGate*. https://www.researchgate.net/publication/384611866

Schneier, B. (2021). *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Springer.

Sharma, D., & Varalakshmi, S. (2024). Analyzing Social Engineering in Cybersecurity. *IEEE Xplore*. https://ieeexplore.ieee.org/abstract/document/10743197/

Tikanmäki, I., & Ruoslahti, H. (2024). Human Factors Make or Break Cybersecurity! *ISIJ*. https://www.isij.eu/system/files/download-count/2024-11/5522_Make_or_break_cybersecurity.pdf

Verizon. (2020). Data Breach Investigations Report. *Verizon DBIR*.

Verizon. (2024). *2024 Data Breach Investigations Report*.