A STUDY OF THE DIFFERENT TYPES OF SOCIAL ENGINEERING ATTACKS AGAINST CUSTOMER SUPPORT OF MOBILE SERVICE PROVIDERS IN MUMBAI

by

RAGISH JAYAPALAN THERAMBIL

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

June 2025

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

< JUNE 2025>

A STUDY OF THE DIFFERENT TYPES OF SOCIAL ENGINEERING ATTACKS AGAINST CUSTOMER SUPPORT OF MOBILE SERVICE PROVIDERS IN MUMBAI

by

RAGISH JAYAPALAN THERAMBIL

Supervised By

Josip Burusic

APPROVED BY

_____

Dissertation chair

RECEIVED/APPROVED BY:

Renee Goldstein Osmic

Admissions Director

DEDICATION

THIS RESEARCH WORK IS DEVOTED TO ALL ENTREPRENEURS WHO OWNES SMALL BUSINESS AND EMPLOYEES WHO HAVE LOST THEIR JOBS BECAUSE OF THE COVID-19.

RESTORATION IS COMING SOON

ACKNOWLEDGMENTS

Throughout my doctoral studies, I have been honoured to receive support from numerous individuals, for which I am deeply appreciative. To begin with, I express my deep gratefulness to God for granting me the strength and perseverance to finalize my doctoral program. During this challenging period, especially amid the Covid-19 crisis, I remained unharmed — a testament to God's unwavering protection.

I am particularly grateful to my academic advisor and research head, Professor Josip Burusic, whose ongoing guidance, insightful feedback, constructive criticism, and steadfast encouragement were instrumental throughout the dissertation process. Your mentorship, Professor, played a crucial role in the successful fulfillment of this scolarly project — it could not have been accomplished without your support from you.

My sincere appreciation also goes to the management and staff of SSBM for providing me the privilege of pursuing my education at such a prestigious business institution. I want to express equal gratitude to all peer doctoral candidates who contributed meaningfully throughout this academic journey.

Additionally, I wish to acknowledge UPGRAD for their thoughtful input and for furnishing valuable case studies from the business school, which significantly enriched the content of this work.

Lastly, I dedicate this academic achievement to the loving memory of my late parents. Their firm encouragement guided me morally as well as enabled me during this doctoral research. Thank you all! May the blessings of God be upon you now.

ABSTRACT

A STUDY OF THE DIFFERENT TYPES OF SOCIAL ENGINEERING ATTACKS AGAINST CUSTOMER SUPPORT OF MOBILE SERVICE PROVIDERS IN MUMBAI

Background

Attacks that involve social engineering have become a significant cybersecurity concern, particularly in the customer support sector of mobile service providers. Unlike traditional cyberattacks that exploit software vulnerabilities, social engineering manipulates human psychology to deceive individuals into revealing sensitive information or performing unauthorized actions. This study explores the various types of social engineering attacks affecting support staff in Mumbai's telecom sector, focusing on techniques such as pretexting, phishing, baiting, and impersonation.

Methods

This study uses a quantitative research methodology based on survey data to thoroughly examine social engineering attacks directed at Mumbai-based mobile service providers' customer support representatives. The research design is based on objective collection of data and statistical analysis for meaningful deductions relating to patterns in attacks, targeted job roles of the employees, and the efficacy of implemented security measures.

Results

The study's findings indicate that attackers often exploit employees' lack of cybersecurity awareness, reliance on scripted procedures, and pressure to provide quick resolutions, making them susceptible to deception. Additionally, the research revealed that stronger security measures and employee training programs can significantly reduce the success of the attacks.

Examination and Conclusion

The study concludes with strategic recommendations for mobile service providers, including enhanced employee training programs, stricter identity verification protocols, and AI-driven fraud detection systems to combat evolving threats. Moreover, the research discusses the role of regulatory frameworks and compliance policies in strengthening cybersecurity defenses. By addressing these vulnerabilities, telecom companies can significantly reduce the risk of attacks based on social engineering and protect both customer data and corporate integrity. This research contributes to the field of cybersecurity by providing actionable insights for industry stakeholders and policymakers.

KEYWORDS

Social engineering, cybersecurity, customer support, mobile service providers, phishing.

Table of Contents

List of Tables

List of Figures

CHAPTER I. INTRODUCTION

1.1 Background of the Research

Human-based engineering attacks—tactics that leverage human behavior rather than exploiting system vulnerabilities—represent a major threat to cybersecurity, especially within the customer service divisions of mobile network providers. The purpose of these schemes is to deceive individuals into disclosing confidential information or performing unauthorized tasks. With a focus on customer service representatives in Mumbai's telecom sector, this study investigates the various social engineering techniques, including pretexting, phishing, baiting, and impersonation. It draws on actual case studies, incorporates perspectives from interviews with sector experts, and assesses current protective measures to identify key weaknesses in customer service protocols (Apruzzese *et al.*, 2019).

The findings reveal that attackers frequently capitalize on employees' insufficient cybersecurity awareness, adherence to rigid procedural scripts, and susceptibility to time pressure. The effectiveness of current security measures, such as multi-factor authentication and knowledge-based verification, in mitigating these risks is assessed **(*An Automated System for Detecting and Preventing Phishing Attempts on Steam Accounts* | *IEEE Conference Publication* | *IEEE Xplore*, no date)**. This study underscores the urgent need for enhanced employee training initiatives, stricter identity verification protocols, and the integration of AI-driven fraud detection systems. It further considers the role of regulatory frameworks and compliance mandates in bolstering cybersecurity defenses. The study concludes by offering strategic recommendations for mobile service providers, encompassing regular security audits, real-time monitoring practices, and simulation-based training exercises (Alzahrani, 2020).

1.2 Problem Statement

The growing occurrence of social engineering attacks targeting customer care personnel within cellular network operations represents a critical cybersecurity challenge. Attackers exploit human vulnerabilities through deceptive tactics like

pretexting, phishing, and impersonation to gain unauthorized access to sensitive customer data. Customer service environments, which routinely handle substantial volumes of personal and financial information, are inherently susceptible to these attacks due to factors such as inadequate authentication methods, insufficient employee training, and the operational pressure for rapid response times. These vulnerabilities facilitate attackers in circumventing security measures, leading to consequences such as SIM card fraud, identity theft, and financial losses. Although security frameworks are already in place, numerous mobile network operators face challenges in successfully identifying and mitigating social engineering threats. This underscores the need for a structured evaluation of attack trends and the performance of existing defense mechanisms. This study seeks to bridge this gap through examinaton of common attack vectors, identifying frequently targeted employee roles, and evaluating the effectiveness of implemented security measures, ultimately generating actionable insights to strengthen customer support defenses and alleviate the risk of social engineering attacks (Rains, 2020a).

1.3 Research Questions

1. What are the most frequently encountered forms of social engineering attacks confronted with customer support teams working in mobile service provider companies in Mumbai?

2. Which employee roles are most frequently targeted in social engineering attacks, and what types of information do attackers attempt to obtain?

3. How effective are the existing security measures in preventing social engineering attacks, and what improvements can be made?

1.4 Research Objectives

- To determine the prevalent types of social engineering attacks targeting customer support teams within Mumbai's mobile service provider industry

- To analyze which employee roles are most targeted and what information attackers try to obtain

- To assess the existing security measures and suggest improvements to prevent social engineering attacks

1.5 Justification of the Study

In the current online era, when economic and personal transactions are on the rise online, data protection of customers has become the most important concern for organizations, particularly mobile network operators. Customer care teams remain likewise important regarding this consideration. They will routinely enumerate sensitive user accounts, enumerate SIM card information, also identify personal information. Social engineering attacks affect the human vulnerabilities, and hence these teams are the best victims for cybercriminals in search of unauthorized access. Understanding the attack methods is required to produce sufficient security measures because traditional cybersecurity tools are often ineffective against deception-based attacks. According to typical attack behavior and most attacked employee positions, the present research gives important data regarding customer support operation vulnerabilities. Better security awareness, application of novel authentication methods, and improvement of incident response procedures serve to improve the level of successful social engineering attacks significantly. Ultimately, this investigation promotes strengthening cybersecurity robustness within the telecommunication sector. Consumer information with the standing of wireless service providers are thus secured.

1.6 Scope of the Study

This study concentrates on Mumbai mobile network operators' customer care teams, which are aimed at social engineering exploits. As a densely populated urban hub with a high concentration of mobile users, Mumbai offers a critical context for examining cybersecurity threats within the telecommunications sector (Korkmaz, Sahingoz and Diri, 2020). Social Engineering in India: Real-Life Scenarios and How to Protect Yourself | LinkedIn, no date). This research specifically aims at how hackers exploit human vulnerabilities within customer support activities, ascertaining most common attack methodologies such as phishing, pretexting, and SIM swap scams. This study probes the distinct varieties of confidential data sought via perpetrators and the predominantly

assailed positions. It also assesses whether present security protocols are efficacious. These steps include authentication procedures besides employee coaching initiatives including incident response strategies for prevention of social engineering attacks. Recognizing vulnerabilities and venturing into fields of potential betterment, the research is working towards providing practicable suggestions towards enhancing cybersecurity in mobile service providers in Mumbai (Conteh and Schmick, 2016).

1.7 Significance of the Study

The following research is meaningful in that it emphasizes serious gaps in the customer support operations of mobile carrier providers, often used through attacks of social engineering. By citing the most common forms of such attacks and their most targeted personnel, this paper sheds illuminate the way of how cyber crooks exploit people to get their hands on otherwise unauthorized customer confidential information. The results augment cybersecurity consciousness within the telecom industry by highlighting enhanced authentication measures, better employee sensitization, and active threat mitigation systems. More importantly, the research has policy-making implications that can inform more effective security measures and compliance solutions for mobile services providers to deter social engineering vulnerabilities. Enhancing security mechanisms in customer support operations will not only safeguard customer information but also build confidence in mobile service providers, ultimately limiting financial losses and reputational loss due to such attacks (‘ED610591.pdf’, no date).

1.8 Theoretical Framework

1.8.1 Social Engineering Theory

Social Engineering Theory describes the ways in which attackers manipulate human behavior to obtain unauthorized access to confidential information. In contrast to conventional cyberattacks that target technical system weaknesses, social engineering exploits the manipulation of people to bypass security procedures. Social Engineering Theory relies on the principles of influence, persuasion, and deception,

where attackers guide with tactics such as impersonation, urgency, and authority to manipulate victims. Social Engineering Theory knowledge helps identify patterns of manipulation used in customer support team attacks, understanding how employees can be better trained to recognize and resist manipulative moves (IEEE Xplore Full-Text PDF:, no date a).

1.8.2 Psychological Manipulation Techniques

Psychological manipulation is the basis of social engineering attacks, relying on cognitive bias and emotional reaction to capitalize on human weaknesses. Attackers leverage weaknesses through tactics such as reciprocity (trading something for something else), authority (by representing a familiar and trusted individual), and social proof (claiming others have complied). Customer support personnel from mobile service providers are specifically at risk because of their function of helping customers, thus tending to take their satisfaction into account above maintaining strict security measures. Organizations can create more effective training programs to enable the employees to identify and reject fraudulent requests once they are aware of such manipulation techniques (IEEE Xplore Full-Text PDF:, no date b).

1.9 Definition of Social Engineering Attacks

The human element remains a key vulnerability in cybersecurity, as technical defenses can be undermined by manipulation or human error. Employees can represent a weak link in security, susceptible to exploitation through unawareness, time constraints, and the inherent inclination to trust. This risk is amplified within customer support, characterized by high interaction volumes and the handling of sensitive data. Enhancing human resilience against these threats requires ongoing security awareness programs, robust authentication protocols, and the cultivation of a security-conscious organizational culture. (IEEE Xplore Full-Text PDF:, no date c)

1.9.1 Explanation of Social Engineering and Its Various Forms

Social engineering encompasses deceptive methods used by cybercriminals to trick people be deceptive methods. Unlike conventional cyberattacks that target

software vulnerabilities, social engineering primarily exploits human psychology, leveraging emotions like trust, fear, urgency, or authority to deceive victims. Attackers utilize diverse manipulation strategies to craft seemingly legitimate requests, thereby inducing employees to disclose confidential information, alter passwords, or grant unauthorized system access.

Impersonation is a common characteristic of these attacks, where perpetrators assume the identity of trusted entities, such as customers, supervisors, IT personnel, or government officials. These tactics exploit the victim's sense of obligation or trust to elicit sensitive data without raising suspicion. Pretexting also features prominently, with attackers fabricating scenarios to lend credence to their requests, often framing them as urgent or critical. Examples include posing as a customer locked out of their account or an IT administrator requiring login credentials for a system update (Aldawood and Skinner, 2019).

Social engineering attacks manifest in various forms, including phishing (deceptive emails or messages prompting clicks on malicious links or disclosure of information), baiting (enticement with rewards to trigger malware installation or credential sharing), and quid pro quo (offering assistance in exchange for information). Tailgating, another prevalent technique, exploits employee helpfulness to gain unauthorized physical access to restricted areas.

To successfully combat these threats and strengthen collaboration within organizations, mobile service providers need to implement effective security protocols to protect the customer support teams. This includes comprehensive employee training on recognizing manipulation tactics, multi-factor authentication (MFA) to strengthen access control, and rigorous verification procedures for handling sensitive customer inquiries. A proactive approach that combines technological safeguards with human awareness is essential for mitigating the risks posed by social engineering (Lansley *et al.*, 2020a).

1.9.2 Comparison with Other Cybersecurity Threats

Social engineering attacks differ from other types of cybersecurity threats in that they do not rely on direct exploitation of program vulnerabilities or weak encryption techniques. Instead, they take use psychology, and thus are harder to detect and prevent using traditional security means. In contrast to malware attacks that use viruses, ransomware, or spyware to compromise systems, social engineering is less about requiring technical hacking skills but more about psychological manipulation. Denial-of-service (DoS) attacks, however, aim to flood network resources to cause service disruptions, while social engineering targets the acquisition of valuable information through manipulation of the employees. Similarly, brute force attacks rely on automated programs to crack passwords, whereas social engineering tactics aim to deceive individuals into willingly sharing their login details (Keserwani *et al.*, 2022).

Social engineering, though varied in form, often accompanies cyberattacks. For instance, a deceptive messsage dispatched via phishing can be embedded with malware that penetrates a system the moment it is opened. Because human error represents a significant vulnerability in cybersecurity, social engineering attacks are often more damaging than purely technical ones, highlighting the need for heightened awareness and comprehensive employee training programs to effectively counter them (Montanez, Atyabi, and Shouhuai, 2022).

1.10 Types of Social Engineering Attacks

Social engineering attacks take the advantage of human psychology for beguiling people so that they reveal private details or provide forbidden access. Many formats represent these assaults via diverse fraudulent strategies for beguiling sufferers. Here are the most popular categories of social engineering attacks:

Phishing

Phishing exists as the most typical furthermore perilous form of social engineering attack, while within it cybercriminals use deceptive emails, text messages, or sham websites for beguiling victims toward revealing private information for instance login credentials, credit card or other personal information. Phishing assaults leverage human reliance as they emulate legitimate institutions like banks, mobile carriers, or governmental departments. Fundamentally, phishing seeks to dupe subjects into divulging private details. People can incidentally select harmful hyperlinks, or they can introduce damaging malware into their systems (Venkatesha, Reddy and Chandavarkar, 2021).

Phishing succeeds because it usually simulates authentic messages, and the attackers utilize logos, common words, and urgency tone to create legitimacy. Scare tactics are the most common strategies, with claims of false data breaches or account access issues used to frighten victims into immediate responses. With a rise in digital communication, mobile carriers have become a frequent target of attack, whereby an attacker would send spam messages in the form of a customer care representative and would ask customers or employees to update account details or change their passwords (Aşan, 2023).

Spear Phishing

Spear phishing is a very personalized type of phishing that targets individual people or businesses. In contrast to generic, mass emails used in phishing attacks, spear phishing attacks utilize the victim's individual information to appear legitimate. Attacker information typically comes from a social media source or a website for the trading and is presented in a form that makes them sound legitimate. For instance, a hacker might impersonate an employee's supervisor, asking for immediate access to a customer's data. Because the email seems to be from a trusted source, the victim will likely agree (Wang *et al.*, 2022).

Whaling

Whaling is a sophisticated variant of phishing that focuses on high-ranking executives such as CEOs, CFOs, and other senior managers. These attacks are

implemented to obtain confidential corporate information, financial records, or executive login credentials. Executives possess access to valuable information, making whaling attacks very profitable for cybercriminals. Attackers usually make messages that purport to originate from regulatory organizations, business allies, or other executives, with a demand for immediate financial operations or confidential documents. Executives, leveraging their authority, might act before confirming the genuineness of the request, resulting in deep security breaches (Hove, 2020).

Smishing (SMS Phishing)

Smishing is a phishing technique conducted through SMS (text messaging). In smishing attacks, perpetrators send deceptive texts that seem to be sent from reliable organizations, urging recipients to click on harmful links, confirm their account information, or contact fake customer support lines. These messages frequently engender a perception of exigency, related to an alert that phone service for the victim shall be severed if immediate responsiveness does not occur. Mobile operators are particularly vulnerable to smishing attacks since the attackers pose as support personnel to gain access to customer account data or initiate SIM card scams. Since SMS messages will be perceived as more intimate and urgent, the victims are more likely to think they are real (Yasin *et al.*, 2021).

Clone Phishing

Clone phishing is a type of attack when the hackers reproduce a legitimate mail that the victim has already received and replace its content with malicious attachments or links. Since the mail appears to be a genuine mail from a trusted person, the victim is likely to open it. In particular, an attacker may copy an official customer service email regarding a recent transaction and replace the original links with phishing links that direct the victim to a spoofed login page. Since the email appears legitimate, the victim

inadvertently enters their credentials, which are recorded by the attacker (Alsufyani and Alzahrani, 2021).

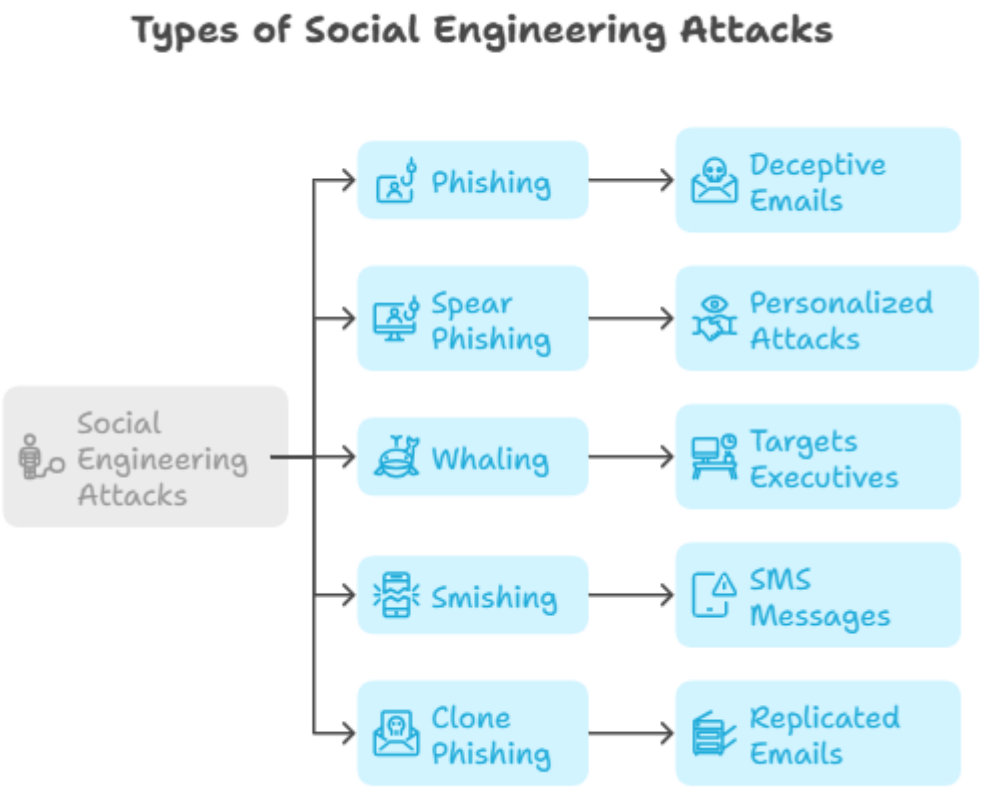

Figure 1. 1: Phishing Techniques

Mitigation Strategies

To avoid phishing, organizations should conduct multi-factor authentication (MFA) to safeguard user accounts, conduct regular training programs for the employees so they can identify attempts at phishing, and install filtering systems in email that can spot and block the suspicious emails. Requesting employees to confirm requests for sensitive information via different channels, e.g., direct phone calls, can also reduce the

probability of becoming a victim of phishing. By remaining alert and implementing proactive security practices, mobile service operators can effectively safeguard their customer care teams and protect sensitive customer information from phishing attempts (Huseynov and Ozdenizci Kose, 2024).

1.10.2 Pretexting

Pretexting is a sophisticated social engineering plan whereby attackers weaves a believable narrative to mislead victims into revealing sensitive data. Phishing involves widespread, indiscriminate impersonation via messages or emails, whereas pretexting depends on direct, personalized interaction with the victim and extensive research of the target's environment to establish trust for the deception. Attackers build a fake persona, say, an IT professional, business manager, or a police officer, and exercise their persuasive abilities to get the victim to reveal secret information or allow unauthorized access (Wang, no date).

This type of attack approach is quite effective as it make use of human psychology over weaknesses in technology. Directives from prominent institutions are often heeded, notably if exigency or legal mandate is spawned. For instance, an assailant could feign being an IT support specialist. They could additionally notify an employee that their account is now vulnerable then solicit login information to "resolve" the problem. Scammers will also pose as top officials and order finance departments to execute wire transfers promptly without undergoing due verification procedures. Another frequent situation is the attackers claiming to be auditors or police officers and asking access to confidential company documents in the guise of investigation.

Pretexting is extremely harmful, especially in sectors that deal with masses of sensitive customer information, like telecommunication and finance. Initially, perpetrators investigate potential victims plus glean intelligence using firm websites, breached repositories, or networking accounts. This data permits them to convincingly impersonate someone. Having gained the victim's trust, they can then get login credentials, financial information, or internal security protocols, which can be used to further exploit (Huseynov and Ozdenizci Kose, 2022).

Mitigation Strategies

Prevention of pretexting attacks occurs through stringent authentication procedures like multi-step authentication processes prior to release of sensitive data. Organizations can incorporate training programs aimed at raising employee awareness to recognize suspicious requests, even when they appear to come from senior officials or known individuals. Adequate verification controls on financial transactions and access to confidential data will also stop fraud in the pretexting. By imposing security-conscious culture and permitting employees to screen unsolicited invitations, companies can actually counter pretexting attacks (Huseynov and Ozdenizci Kose, 2022).

1.10.3 Baiting

Baiting is a sneaky social engineering attack predicated on exploiting individuals' greed, curiosity, or need for free prizes to trick victims into offering security in return. While phishing primarily relies on the utilization of impersonation of an official email or notice to deceive users, baiting fulfills its purpose by the offering of something attractive—free software applications, movie downloads, or gift certificates—to lure victims into actions that expose their systems or personal data to risk. The general concept behind baiting is to have the victim willingly engage with an apparently harmless offer without realizing that they are essentially dealing with a security risk.

The most prevalent baiting attacks are with malicious USB drives. Malicious cyber attackers place infected USB drives in areas where people frequently pass, for example business parking lots, coffeehouses, or restrooms, in the hope that a victim will pick one up and insert it into their system out of curiosity. The malware is installed upon insertion, and the cyber attackers have access to sensitive data, keystroke logging, or full control over the system from the remote end. This method has been used successfully in business espionage and mass-scale cyber attacks to demonstrate how something as harmless as curiosity can lead to disastrous security violations.

Another common type of baiting is fake software downloads, where attackers mimic legitimate programs, music releases, or movie downloads. The attacking victims

in pursuit of free access to good content unknowingly install malware, which can steal their credentials, monitor their activities, or offer unauthorized access to intruders. Similarly, baiting can be achieved through web-baiting, where phishing sites provide exclusive offers, e.g., free phone or coupons, for completing forms with personal information. After the victim has entered their details, attackers can use them for identity theft, financial fraud, or phishing attacks.

Baiting is so effective due to human psychology, as victims are tempted with the potential reward while keeping the risks involved low. It is not on most people's minds to question the legitimacy of a free offer or the risks involved in messing with unknown computer files. To avoid baiting attacks, businesses must have strict cybersecurity in place, i.e., shut down USB ports on business machines, avoid unapproved software downloading, and educate employees on the danger of being too-good-to-be-true offers. Companies can also use endpoint security solutions to identify and block malware infection from unauthorized software or hardware. By creating a culture of suspicion and awareness in cybersecurity, individuals and organizations can reduce their exposure to baiting attacks to the maximum (Chebii, 2021).

1.10.4 Quid Pro Quo

Quid pro quo, namely "something for something" in Latin, constitutes a social engineering assault whereby the assurance of aid, a gain, or a utility deceives targets for private details. Quid pro quo attacks, dissimilar to baiting, include a pledge for assistance or assistance to the victim, coupled with the trick appearing more authentic coupled with credible since baiting hinges upon concrete benefits for example free software or gifts. Cybercriminals manipulate human psychology with specific regard to the inclination toward reciprocation. Subsequently, sufferers are inclined to offer confidential data or admittance to fortified networks.

A common example of a quid pro quo attack involves fake tech support calls, where cybercriminals impersonate IT personnel and tell victims they are addressing a technical issue. They may contact an employee, claim to have found a problem on their computer, and request remote access credentials to ‘fix’ the issue. With access already granted,

the intruder can steal information, install malware, or even lock the users out of their own systems. Several high-profile breaches have been caused by insiders inadvertently providing credentials to attackers posing as authorized IT staff.The second most used method is survey scams, wherein the fraudsters ask individuals to fill out a survey for which they will be rewarded with cash, gift cards, or discounts. The victim is asked to provide their personal data like email address, phone number, or even bank information to get the reward. These are then used for financial scams, phishing, or identity theft. Since people are ready to do surveys for something in return, they will not suspect that the request is fake (Mihretu *et al.*, 2023).

Another focused quid pro quo attack is the job offer scams, where attackers pose as hiring managers with enticing job offers. They lure victims into providing their personal details such as Social Security numbers, passport photocopies, or bank details in the guise of recruitment or upfront deposits of wages. Even victims are asked to pay for background checks or training certificates beforehand, only to realize later that the job opportunity was fake.

Quid pro quo attacks are effective because they exploit trust and the natural human tendency to respond positively when offered help or an opportunity. Organizations and individuals need to be watchful to thwart these attacks, to validate the authenticity of unsolicited assistance, not to send confidential data by phone or email, and to move slowly in reacting to too-good-to-be-true situations. Periodic employee training on social engineering methods and implementing strict security practices such as multi-factor authentication and authentication protocols can effectively reduce the chances of falling victim to such attacks (Hussain, Siddiqui and Islam, 2023)

1.10.5 Tailgating

Tailgating or "piggybacking" is a kind of social engineering attack that uses human behaviour to obtain unauthorized physical access to protected areas. Unlike web-based cyberattacks targeting system vulnerabilities, tailgating exploits psychological manipulation and social conventions such as politeness and trust. There are several techniques employed by attackers to make authorized personnel let them pass without

security screening, without any hacking and technical expertise. Since most organizations pay greater attention to digital security and overlook physical security, tailgating remains a serious threat, particularly in working environments where workers repeatedly enter and exit secured spaces.

The most common form of tailgating is probably when an attacker has large loads or is having trouble and, through good intentions, a sympathetic worker leaves the door ajar for them. Workers assume the individual is a co-worker or individual who has business in the building. Another common scam involves attackers posing as delivery staff, exploiting the routine visits of couriers to office buildings. Because employees often do not question delivery personnel, these attackers can easily blend in by wearing uniforms or carrying packages, allowing them to access restricted areas undetected.

Also, tailgating is possible when an attacker pretends to be an employee who has "forgotten" their access card and asks another person to give them the access. This is effective especially well with large organizations where employees don't know everyone, consequently it is simplier for attackers to gain entry by pretending to be new hires or contractors. The attacker can thus steal confidential documents, inject malware into unlocked computers, or view confidential information without in the process sparking immediate suspicion.

Tailgating poses a significant security risk, as it allows attackers to bypass protective measures with ease. Unlike hacking, which demands technical expertise, this tactic relies solely on exploiting human behavior and social norms. To neutralize the threat of tailgating, organizations have to enforce rigid access control regimes like requiring employees to individually swipe their access cards and preventing unauthorized users from entering after them in. Besides, training of staff concerning awareness about detection and prevention from such attacks must be carried out to make workers aware of them. Organizations should also implement the exploit of biometric authentication technologies, security turnstiles, and CCTV to guarantee that only the authorized people enter the closed areas.

Social engineering methods— including phishing, pretexting, baiting, quid pro quo, and tailgating—rely on psychological manipulation rather than exploiting technical flaws. Mobile services customer care operators are most vulnerable as they handle customers on a daily basis and have to handle confidential data. All these attack modes should be familiar with proper security measures like stringent authentication techniques, well-trained staff, and vigilant monitoring for prevention and detection of malicious access and data loss (Naz *et al.*, 2024).

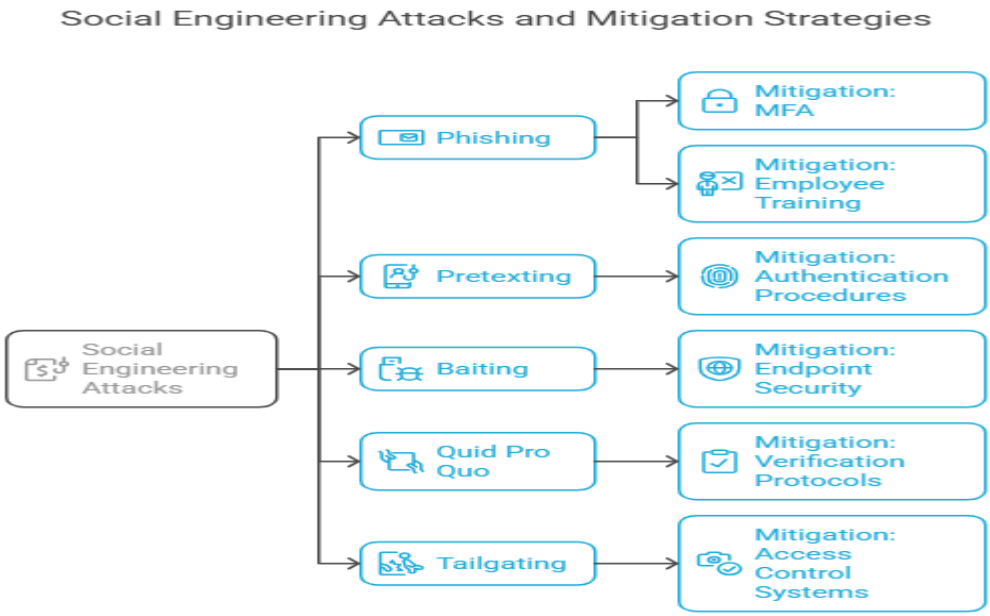

Figure 1. 2: Social Engineering Attacks

1.11 Methods Used by Attackers in Customer Support Attacks

Social engineering cyber attacks against customer support teams obtain unauthorised access to sensitive data by abusing human contacts and technical weaknesses. Cyber attackers apply different strategies to deceive workers and compel them to share sensitive information or give access to enterprise systems. Outlined below are several widely used tactics employed in attacks targeting customer service teams.

1.11.1 Email and Phone-Based Attacks

Phone and email scams are among the most frequently used social engineering strategies cybercriminals employ to deceive customer support personnel. These attacks access sensitive information via system vulnerabilities plus human interactions. Hackers employ a wide range of techniques to manipulate employees and compel them to provide confidential data or give access to company systems

Phishing Emails

Phishing emails are misleading messages designed to impersonate authoritative sources, such as company managers, IT staff, or regulatory bodies. They often contain fake invoices, password reset requests, or menacing security alerts that lead employees into taking immediate action. Malicious attachments or links are added by attackers to these emails, which, when clicked or downloaded, can infect the system with malware, steal login credentials, or redirect victims to imposter websites that collect sensitive information.

Spear Phishing

Unlike widespread phishing campaigns that target large groups, spear phishing is a highly focused attack. Cybercriminals carefully research their victims beforehand, using publicly available information from platforms like LinkedIn, company websites, or social media to craft convincing and personalized messages. For example, the customer service agent might receive an email appearing to be from their manager or IT department asking them to reset a customer's password or recapture payment information. Since these emails include tailored details and professional terminology, employees are more vulnerable to deception.

Vishing (Voice Phishing)

Vishing, short for voice phishing, involves attackers making phone calls while impersonating legitimate individuals such as customers, IT staff, or company executives. These aggressors can make up an atmosphere of urgency by alleging they have identified some unauthorized activity or an account must be verified instantly. Customer care

service representatives, feeling stressed, might not even realize they are sharing sensitive information like account information or customer verification points. Other attackers also employ caller ID spoofing with the aim of having their numbers displayed as authentic, further tricking the victim.

Smishing (SMS Phishing)

Smishing is a phishing attack conducted via SMS (text messages). Attackers send fraudulent messages to customer support groups, pretending to be in-house departments, banks, or security groups. These messages usually include harmful links or commands to dial an artificial helpline, where attackers masquerade as company representatives and extract sensitive information. Because SMS messages are regarded as credible, the victims can be less wary while reacting (Hadikusuma, Lukas and Rizaludin, 2023).

Impact and Prevention

- These attacks can lead to data breaches, financial loss, and reputational damage for organizations. To reduce risks, organizations ought to:
- Use email filtering and anti-phishing tools to detect and block suspicious emails.
- Customer service personnel must be provided with regular cyber security training so that they identify attempts at phishing, vishing, and smishing.
- Lock accounts through multi-factor authentication (MFA) if the credentials are probable to have been stolen.
- Implement rigorous verification processes to identify customers and orders from within first before revealing sensitive information.
- With becoming more vigilant and implementing strict security practices, organizations can protect their customer service staff from phone and email attacks.

1.11.2 Impersonation Tactics

Impersonation is a common tactic in social engineering attacks, where attackers pretend to be someone they are not to manipulate customer support agents into

providing unauthorized access or information. This method exploits the natural tendency of employees to be helpful and cooperative.

- **Pretending to be a Customer**: Cybercriminals contact customer support via phone or email, falsely stating that they have been locked out of their account. They use social engineering techniques such as providing partial information (e.g., a real customer's name and address) obtained through data leaks or online research. They then convince the agent to reset passwords, issue new SIM cards, or provide confidential account details.

- **Posing as an Internal Employee**: Cybercriminals may impersonate IT staff, managers, or security personnel and request sensitive company data. For example, an attacker might call a customer support representative, claiming to be from the IT department, and ask for login credentials under the pretense of performing "urgent maintenance."

- **CEO Fraud (Business Email Compromise - BEC)**: Attackers send emails impersonating senior executives, requesting sensitive information or urgent actions. For example, an email appearing to be from the company's CEO might instruct a customer support manager to approve a wire transfer or release confidential customer data.

- **Fake Service Providers**: Cybercriminals may pose as external vendors or auditors conducting security checks and request access to internal systems, databases, or customer records.

1.11.3 Exploiting Internal Systems and Processes

Adversaries prefer targeting internal security policy vulnerabilities, procedure vulnerabilities, and software vulnerabilities with an aim at impacting customer support staff. Knowledge of the systems and how one goes about accomplishing things, they identify loop-holes by which they get information or make access.

Imposing Password Reset Processes: Most mobile operators have password reset security questions or authentication processes. The hackers obtain personal details

from social networking sites, database breaches, or phishing to input the solutions to these questions appropriately, hence allowing them to hijack customers' accounts.

Misusing Two-Factor Authentication (2FA) Bypass: Some attackers trick customer support representatives into disabling 2FA or sending authentication codes to new email addresses or phone numbers claiming to be a "lost device."

SIM Swapping Attacks: In SIM swap fraud, hackers trick customer support personnel into porting a customer's number to a new SIM card that is in the possession of the attacker. The attacker can intercept calls and SMS messages, which include one-time passwords (OTPs) for bank transactions and internet accounts.

Taking Advantage of Insider Threats: Attackers sometimes bribe or collaborate with employees to gain access to internal systems. Malicious insiders may be hired to steal customers' data, disable security measures, or approve fraudulent transactions.

Adversaries prefer targeting internal security policy vulnerabilities, procedure vulnerabilities, and software vulnerabilities with an aim at impacting customer support staff. Knowledge of the systems and how one goes about accomplishing things, they identify loop-holes by which they get information or make access.

Attackers use a mixture of email and phone-based deception, impersonation tactics, and system exploitation to manipulate customer support teams in mobile service providers. Understanding these methods is critical for strengthening security protocols, training employees, and implementing multi-layered authentication processes to prevent unauthorized access and data breaches.

1.12 Employee Roles Most Frequently Targeted

Social engineering attackers often target specific employee roles within customer support teams based on their level of access to customer accounts, internal systems, and sensitive information. Understanding which employees are most frequently targeted and why helps organizations implement role-specific training and security measures to mitigate risks. The following are the key roles most vulnerable to social engineering attacks.

1.12.1 Customer Service Representatives

Customer service representatives (CSRs) form the front line of clients, who address a multitude of questions, complaints, and services requests. Direct contact with customers and privileged account information, they are the priority target for social engineering. Social engineers exploit the courteous, friendly, and accommodating nature of CSRs and practice deception and manipulation to win the trust of the CSRs to provide unauthorized access, modify customer accounts, or deliver confidential information.

Why CSRs are Hacked

CSRs receive huge numbers of customer calls on a daily basis, making it possible for hackers to go unnoticed easily among genuine customers and conduct fraud without their account being flagged on suspicion. Their ability to modify accounts, such as billing information, to reset passwords, and SIM card activations makes them vulnerable entry points to those who would like to hijack customers' accounts or make unauthorized transactions. Perpetrators use pressure and urgency tactics as well, such as pretending to be an anxious customer whose account has been hacked or an executive who needs immediate access to an account. WUnder intense pressure, customer service representatives may unintentionally overlook verification procedures, heightening the risk of unauthorized access (Wang, Zhu and Sun, 2021a).

Typical Attacks on CSRs

Phishing emails are probably the most widespread social engineering attack against CSRs, whereby attackers masquerade as managers, IT support, or security personnel and email the CSRs asking them to take immediate action, like verifying login credentials or changing passwords. The emails may contain malware attachments or links which, once opened, can download malware or lead to credential leakage. Another frequently used tactic is vishing, or voice phishing, where attackers call customer support posing as genuine customers claiming account access issues. They often use caller ID spoofing to make their number appear legitimate, and so the CSR again provides unauthorized access

Another advanced attack technique is pretexting, whereby attackers create authentic pretexting situations to deceive CSRs. For instance, an attacker might impersonate a law enforcement officer or regulatory body and claim that they require customer information for an active investigation. With forged credentials or case numbers, they build their request to appear authentic, deceiving CSRs into divulging sensitive customer information without adequate verification (Prabhu Kavin *et al.*, 2022).

Preventing Social Engineering Attacks

In counteracting these risks, organizations should possess robust authentication procedures, frequent employee training, and strict verification procedures. CSRs must undergo training on the social engineering tricks, be informed to authenticate each request carefully, and be given instructions to escalate unusual interactions ahead of taking actions on them. By making the employees security savvy and vigilant against unusual customer behaviors, companies are able to protect their customer support personnel from being victims of social engineering attacks as well as keep unauthorized parties away from customer accounts.

1.12.2 Technical Support Staff

Technical support staff play central roles in supporting the IT setup of an organization through repairing networks, debugging malfunctioning hardware, patching software, and configuring security levels. As their uncontrolled backend access, their diagnostics kit, and admin commands set their potential impact, technical support staff become first choice targets for cyber thieves. They exploit their high access level for hijacking inner computers, claiming corporate data, or customising security to future threats

Why Technical Support Teams Are Targeted

Among the principal motives why technical support staff are targeted are that they have access to internal systems and can alter system settings, reset security settings, and assign extra service rights. In the event of a breach, the intruder has the capability to employ this access to go around security settings, enable destructive capabilities, or

steal important information. On top of that, these teams will also manage private company data such as software updates, business security configuration, and levels of vulnerabilities. This data will be helpful to attackers that are targeting firms with a desire to release unchecked vulnerabilities or construct sophisticated malware tailored to the company's environment.

The second critical consideration is the reliance by other staff members on technical support staff. As tech support staff are expected to provide assistance in security and IT-related matters, employees may not want to ask for authentication of requests that seem to be coming from them. Attackers take advantage of this by posing as the tech support team, phoning or emailing employees stating they have seemingly genuine requests for logins, access to systems, or security patches.

Common Technical Support Staff Attacks

The most frequent attack technique is impersonation, where cybercriminals pose as company representatives or IT administrators who need immediate access to internal networks or customer accounts. These requests are employed to establish a sense of urgency to compel tech support personnel into compliance without adhering to proper confirmation protocols. Another perilous attack is malware injection, wherein attackers deceive tech support staff into installing harmful software packaged as a required system upgrade or security update. The malware, having been installed, can steal data, monitor keystrokes, or create backdoors that can be opened up for future exploitation.

Malicious security incident reports are being used to trick technical support staff. Malicious users create spurious cybersecurity threats and orchestrate a sense of severe security breach that demands immediate response. This is being used to trick support staff into approving unauthorized access, disabling security measures, or exposing confidential data on the company defense networks.

Preventing Social Engineering Attacks

To counter these weaknesses, the organizations would have to implement stringent authentication, wherein all internal requests receive authentication via

redundant channels prior to granting access. Security training conducted on a periodic basis should make the tech support employees aware of learning social engineering methods like fake urgency, out-of-context asking, and impersonation attacks. Logging and monitoring of access requests should also help in anomaly detection and prevention of unauthorized manipulation of critical systems. Through enhancing security awareness and enforcing rigorous access control, organizations can effectively reduce the risk of social engineering attacks on technical support teams.

1.12.3 Managers and Supervisors

To counter these weaknesses, the organizations would have to implement stringent authentication, wherein all internal requests receive authentication via redundant channels prior to granting access. Security training conducted on a periodic basis should make the tech support employees aware of learning social engineering methods like fake urgency, out-of-context asking, and impersonation attacks. Logging and monitoring of access requests should also help in anomaly detection and prevention of unauthorized manipulation of critical systems. By improving security awareness and implementing strict access controls, organizations can significantly lower the likelihood of social engineering attacks targeting technical support teams.

The greatest reason attackers focus on targeting managers is that they possess their high-level access, which entitles them to have administrative responsibility over customer accounts, internal process flows, as well as the company's rules. They are the most vulnerable entry points for attackers looking to gain access to sensitive data. Secondly, managers can override security controls, including bypassing multi-factor authentication (MFA) or changing account access permissions, which attackers take advantage of by creating false and apparently legitimate request scenarios. Workload and distractions under which managers operate on a daily basis create another weakness. Performing multiple tasks simultaneously can make them approve requests in haste without proper scrutiny, which exposes them to security failures.

Among the most effective social engineering attacks directed at managers is Business Email Compromise (BEC), where the cybercriminals act as executives,

business partners, or internal departments to trick managers into receiving false payments or exposing sensitive information. Another such attack is CEO fraud, where cybercrime actors impersonate top executives and send high-priority emails requesting fund transfer, security credential reset, or unauthorized access approvals. Since these requests seem to be coming from senior officers, managers can comply without questioning their validity. Second, the cybercriminals exploit inner policies by inducing managers to authorize exceptions to usual security procedures, e.g., resetting passwords with partial authentication or turning off security controls for "operational convenience" on an interim basis.

Customer service representatives, technical support personnel, and managers are the most common targets of social engineering attacks on mobile carriers. The hackers take the advantage of their privileges, access levels, and psychology to make them bypass security controls. Discovery of these vulnerabilities is essential for organizations to adopt stricter security procedures, focused training programs, and stricter verification processes. By promoting awareness, multi-layered authentication, and well-defined guidelines for processing sensitive requests, businesses can halt the threats of social engineering attacks, and in the same time protect their employees and customers against cyber attacks.

1.13 Commonly Exploited Information in Social Engineering Attacks

Social engineering attacks against customer service operations are aimed primarily to acquire sensitive data that will be used in fraud in financial systems, identity fraud, or unauthorized access to telephone networks. Malicious actors trick employees into divulging confidential information with minimal or no knowledge of its security implications. The most prevalent forms of information sought in the attacks are as follows:

1.13.1 Customer Personal Data

To counter social engineering attacks, which commonly exploit customer support teams to obtain customer personal data, SIM card details, and internal system credentials through deception, impersonation, and manipulation, it is critical to

implement strong authentication procedures, increase employee awareness, and enforce strict access controls(Mouton, Leenen and Venter, 2016).

1.13.2 SIM Card and Account Details

SIM swap fraud is among the most severe social engineering attacks targeting mobile service providers. In this scam, attackers deceive customer support staff into transferring a victim's phone number to a SIM card they control. This enables cybercriminals to intercept calls, emails, and critical one-time passwords (OTPs), granting them entry to the person's banking, social media, email, and other digital accounts. Because the customer care employees of mobile network operators are responsible for SIM activation, replacement, and changes in account, they are the ones most at risk from cybercriminals who use deception and threats to bypass security controls.

Fraudsters go after all types of SIM-related data to perpetrate their fraud activities. They go after, for instance, the SIM Card Number (ICCID), a unique SIM card identifier, and utilize it to request unauthorized SIM changes by providing false reasons such as "lost or damaged SIM cards." They also take over mobile numbers and account PINs, which enable them to gain direct access to customers' accounts or bypass security checks. Besides, call and SMS records are valuable for attackers to use for espionage, blackmail, and even social engineering against third parties. Further, the IMEI number and device details on a victim's mobile phone can be utilized to track the victim's location or to perform further fraud, for instance, cloning a victim's phone.

The biggest misuse of such compromised information is through SIM swap scams, whereby the hackers coerce customer support operators into transferring a victim's number to a new SIM operated by them. This gives the attacker full access to incoming calls and messages, thereby hijacking the victim's phone identity. Once they get hold of the victim's phone number, they perform account takeovers by initiating password reset on bank apps, social media platforms, and email services. The majority of such services use the registered phone number of the victim to regain their account and authenticate OTP, thus making SIM swap fraud a very powerful attack tool. With complete dominion

of the victim's online identity, thieves can steal funds, freeze victims out of their own accounts, or even pretend to be them to fool friends, family members, or business partners (Salahdine and Kaabouch, 2019a).

With the severe intensity of the SIM swap fraud penalties, the mobile network operators must install robust security features to avoid unauthorised SIM swaps and account changes. Customer verification processes must be more stringent, multi-factor authentication (MFA) must be employed, and routine employee instruction must be instituted to preclude these menaces. Patrons also require instruction concerning the manner in which they are able to protect private details. Patrons should likewise disclose deceitful dealings coupled with employing authentication applications in lieu of SMS-based verification wherever feasible. Identifying and disabling SIM-related fraud threats is crucial to safeguarding businesses alongside with individuals from catastrophic cybercrime.

1.13.3 Internal System Credentials

Internal system credentials like customer care portal login, admin tools, and remote access solutions are some of the most exploited assets by cybercriminals targeting mobile operators. The illicit access enables the hackers to play around with customer accounts, produce fake SIM replacements, change billing data, and even cut down crucial services. Because mobile carriers process enormous amounts of private information, the internal support infrastructures are valuable targets for phishing, malware, and impersonation attackers seeking to gain authentication credentials and evade security controls. Intruders achieve forbidden entrance into consumer databanks. Then they are able to pilfer sizable amounts of personal information such as names, addresses, credit card numbers, and government identification details.

Compromised data can be advertised for sale on black markets or used to commit identity theft, financial fraud, and phishing attacks against customers. The second significant threat posed by stolen internal credentials is insider attacks. Because the attackers can obtain access to the special account of an employee, they are able to elevate privileges and sabotage lower layers of the company's security infrastructure.

This can result in enormous information breaches, service downtime, or even ransom attacks in which the hackers crash vital systems and demand ransom in exchange for removing the blocks. Additionally, the breached accounts may be exploited to send organization-wide phishing emails aimed at harvesting further credentials or conducting harmful activities.

To safeguard against such hazards mobile carriers must institute strong security procedures. These provisions must shield important credentials against forbidden access. Key strategies include adopting multi-factor authentication (MFA), applying role-based access controls (RBAC) to limit user privileges, and monitoring login activities for unusual behavior. Additionally, ongoing employee training to identify phishing and social engineering attempts aimed at stealing credentials is essential. Through securing authentication processes, restricting privileged access and improving cybersecurity culture, mobile carriers can easily eliminate the chance of inner credential-stealing and its devastating impact (Heartfield and Loukas, 2015a).

Personal customer data, SIM card information, and internal system credentials are among the most frequently targeted assets in social engineering attacks against mobile service providers. Attackers use deception, impersonation, and manipulation to extract these details from customer support teams. Strengthening authentication processes, increasing employee awareness, and implementing strict access control measures are crucial in mitigating these risks.

1.14 Security Measures in Place

In social engineering attacks targeting mobile service providers, the most frequently compromised information includes customers' personal details, SIM card information, and internal system access credentials. Attackers obtain this data by deceiving, impersonating, and manipulating customer support personnel. Strengthening authentication processes, enhancing staff awareness, and enforcing rigorous access restrictions are essential measures to mitigate these risks (Airehrour, Vasudevan Nair and Madanian, 2018).

1.14.1 Authentication and Verification Protocols

Security of customer data heavily relies on authentication methods like Multi-Factor Authentication (MFA), Knowledge-Based Authentication (KBA), and biometric confirmation. Nevertheless, attackers exploit human error and poor implementation. Mobile providers must continuously update these protocols and enforce strict verification even under pressure situations (Aun *et al.*, 2023)

1.14.2 Employee Training Programs

Thorough training and awareness programs for employees are crucial for mobile service providers to successfully guard against social engineering threats. Given that these attacks target human psychology rather than technical weaknesses, employees serve as the first line of defense against deceptive attempts to obtain illegal access to accounts or internal networks. Attackers employ various psychological tactics, including deception, time pressure, or emotional manipulation, to induce employees to bypass security protocols. Consequently, poor training may cause employees to unintentionally reveal confidential information or provide unauthorized access, putting both customer data and the organization's security at risk.

A well-structured employee training program should encompass several key areas to cultivate strong security awareness. Foundational to this is education on social engineering methodologies, equipping employees to identify common manipulation techniques used by attackers. This includes recognizing impersonation attempts, fabricated urgency, and the exploitation of personal information gathered through phishing or social media. Phishing simulation exercises also constitute a valuable training component, allowing employees to practice identifying and responding to realistic phishing scenarios in a controlled environment. These simulations can help reinforce best practices and correct any risky behavior

1.14.3 Incident Reporting Systems

Effective incident reporting systems with real-time monitoring, alert mechanisms, and trained response teams are essential. They enable organizations to quickly detect, analyze, and respond to social engineering threats, minimizing damage (Bhusal, 2021).

1.15 Lack of Consistent Training Programs

Authentication systems, while a primary defense preventing illegal access, stay vulnerable to social engineering. Attackers often bypass these systems by exploiting human administrators or using stolen personal data. A key weakness is the over-reliance on Knowledge-Based Authentication (KBA), where security questions use easily obtainable static data like birthdates or addresses, rendering them ineffective. SIM swap fraud also presents a critical risk, as attackers can manipulate support staff to transfer a victim's phone number, intercepting SMS-based One-Time Passwords (OTPs). Furthermore, inconsistent enforcement of security policies, where customer care staff prioritize speed over security, creates exploitable vulnerabilities.

To counter these weaknesses, mobile operators must strengthen Multi-Factor Authentication (MFA) with biometrics or token-based authentication, which are harder to compromise than traditional KBA. AI-driven fraud detection can also identify anomalous login attempts. Crucially, stringent enforcement of authentication protocols through consistent employee training is essential.

Addressing these authentication vulnerabilities is crucial for mobile operators to reduce account takeovers and SIM swap fraud. A robust authentication system, combining enhanced MFA, AI-driven fraud detection, and strict security enforcement, is vital to safeguard against social engineering attacks and protect customer data and network integrity (Gragg, 2003)

In addition, numerous organizations lack adequately staffed incident response teams, resulting in slow reactions to social engineering breaches. Such delays give attackers additional time to expand their access, infiltrate more accounts, and cover

their tracks. To mitigate this, organizations must prioritize real-time threat detection using AI-powered security monitoring, automated alerts, and behavioral analytics to identify and respond to abnormal activity promptly.

Ultimately, bolstering defenses against social engineering necessitates addressing vulnerabilities in authentication, employee training, and incident response. Mobile carriers must adopt a proactive security posture that includes stronger authentication, continuous employee education on evolving threats, and streamlined incident response procedures, ensuring the protection of customer data and maintaining operational resilience.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

The Indian telecommunication industry is experiencing rapid growth, driven by increasing mobile and internet usage, government initiatives like Digital India, and liberalized FDI policies. This expansion has contributed to an increase in cybersecurity risks, especially social engineering attacks that manipulate human behavior to mislead victims. Cybercriminals employ tactics like phishing, fraudulent phone calls, and impersonation schemes to target both users and customer service personnel, potentially resulting in financial fraud, identity compromise, and unauthorized access to private information.

Although social engineering attacks are becoming increasingly common in the telecommunications sector, most existing research emphasizes technical system flaws, while the human factor in security breaches remains largely overlooked. Conventional security approaches frequently fail in handling with these risks, underscoring the urgency for a thorough investigation into attack methodologies and the formulation of targeted defense strategies. This dissertation aims to deal with this gap by evaluating various social engineering attack methods, and it pinpoints deficiencies in customer care processes, and it gauges the efficacy of current security practices among mobile network operators. We principally aim for practical guidance and calculated counsel. Such actions shall fortify cybersecurity defenses also augment the telecommunications industry's durability.

Paimin et al. (2016) demonstrate that spear-phishing, which leverages detailed personal information to craft convincing messages, is more effective than general phishing, indicating the value of tailoring attacks to individual beliefs and intentions.

Workman (2008) provides empirical evidence that greater user awareness, a key component of attitudes, improves the detection of phishing attempts.

Nicholson, Coventry, and Briggs (2017) show how easily attackers can create fake online personas to infiltrate networks, underscoring the influence of perceived social norms and trust on susceptibility.

Wang, Zhu, and Sun (2021) point out that social engineering takes advantage of human weaknesses, revealing the shortcomings of security approaches that focus solely on technology while overlooking how user beliefs and intentions influence behavior."

2.4 Impact of Social Engineering on Mobile Service Providers

Table 2. 4:Social Engineering Threats and Their Impact in a Digital Society

Author(s)	Method Used	Advantages	Limitations
Salahdine and Kaabouch (2019b)	Literature review on the increasing rate of social engineering attacks in modern networks	Highlights social engineering as a major cybersecurity weak link and explains why technical defenses (firewalls, antivirus, etc.) are ineffective	Lacks empirical data or case studies to validate claims
Hijji and Alam (2021)	Theoretical analysis of social engineering as a psychological tactic	Provides insights into how attackers exploit human trust rather than system vulnerabilities	Does not present quantitative data or real-world incident analysis

(Hantrais and Lenihan, 2021)	Report analysis from cybersecurity firms and government agencies	Uses real-world statistics (e.g., Cyence report, DOJ assessment) to quantify financial impact	The information might be obsolete, and the research lacks concrete recommendations for mitigation.
Pokrovskaia and Snisarenko (2017)	Case study of phishing-based social engineering attack on a financial institution	Demonstrates the high stakes of social engineering attacks in real-world financial systems	Focuses on a single incident; does not generalize findings to other industries or types of attacks
Mahanama, Shirvani, and Rachev (2021)	Observational analysis of attack stages (reconnaissance, rapport-building, exploitation, cover-up)	Breaks down the methodology of social engineering, allowing for a structured understanding	Does not propose a defense framework beyond generic strategies like employee training

Table 2. 5:Phishing and Spear-Phishing Techniques, Detection Methods, and Countermeasures

Author(s)	**Method Used**	**Advantages**	**Limitations**
Hawa Apandi, Sallim, and Mohd Sidek (2020)	Literature review on phishing attacks and countermeasures	Provides a broad classification of phishing attacks and highlights deep learning as a future research direction	Lacks empirical validation or testing of proposed detection methods
Adil et al. (2020)	Theoretical analysis of phishing threats in modern digital services	Covers multiple attack vectors and security measures, emphasizing intrusion detection systems (IDS)	Does not propose or evaluate novel anti-phishing mechanisms
Qin and Burgoon (2007)	Survey-based study on phishing	Highlights the importance of user	Relies on self-reported awareness,

	awareness and detection	education and real-time detection mechanisms	which may not reflect actual user behavior
Alabdan (2020a)	Literature review and analysis of traditional and modern phishing techniques	Identifies emerging phishing tactics like QR code phishing and voice phishing	Lacks experimental validation or proposed countermeasures beyond awareness
Zamir et al.(2020)	Stacking model-based machine learning approach for phishing website detection	Uses advanced feature selection techniques (RFE, PCA) and achieves 97.4% classification accuracy	Requires further validation in real-world environments
Mohammad.et.al (2021)	Investigation of ensemble learning and feed-forward neural networks for phishing detection	Enhances classification accuracy using PCA-selected features and stacked classifiers	Needs real-time validation and exploration of additional feature extraction methods

Table 2. 6: Summary of Studies on Social Engineering, Behavioral Interventions, and Customer Service Automation

Author(s)	**Methodology**	**Limitations**	**Advantages**
Conteh and Schmic(2021)	Review of cyber threats and social engineering attacks, proposing security measures	Cannot definitively confirm if training programs always yield results due to limitations in Columbia College research	Comprehensive discussion on social engineering, identification of psychological vulnerabilities, and emphasis on awareness programs
Prentice and Paluck (2020)	Examination of social norms as behavioral interventions, focusing on	Conceptual and practical complexities in applying social norm research to real-world interventions	Highlights the effectiveness of social norms in behavioral change and offers a framework for

	messaging and group dynamics		integrating them into interventions
Vande Velde, Overgaard, and Bastien (2021)	Comparative analysis of social-norm interventions and traditional "nudge-based" psychological methods	Limited in practical application to specific case studies rather than broad implementation	Demonstrates how group dynamics can enhance behavioral interventions more effectively than classic psychological tactics
Xiao and Kumar (2021)	Conceptual framework analyzing the drivers and consequences of adopting robotics in customer service	Framework primarily theoretical and lacks empirical validation in real-world scenarios	Provides management recommendations for integrating robotics into customer service and examines factors influencing automation acceptance
Ragno et al.(2023)	Survey-based quantitative analysis using regression, correlation, and covariance evaluations	Limited by a lack of existing literature, making it difficult to provide conclusive results	Provides practical insights into service quality, customer satisfaction, and loyalty across diverse ethnic and professional groups

Table 2. 7: Summary of Studies on Impersonation Techniques and Their Impact on Customers

Author(s)	**Method**	**Limitations**	**Advantages**

Lee et al. (2020)	Machine Learning-based IDS for cyber-physical-social systems.	High computational power requirement makes it unsuitable for IoT devices.	Effective intrusion detection in large-scale networks.
Maldonado, Riff, and Neveu (2022)	Lightweight IDS using deep autoencoder and C4.8 wrapper for feature reduction.	May not generalize well to diverse network environments.	High accuracy (98.22%) and low false alarm rate (1.20%) on AWID dataset.
Campobasso and Allodi (2020)	Investigation of IMPaaS criminal infrastructure and MFA bypassing.	No direct mitigation strategies proposed.	Provides evidence of large-scale impersonation-as-a-service operations.
Siwakoti et al (2024)	Case study of Russian IMPaaS platform with over 260,000 user profiles.	Focuses on a specific underground market, limiting applicability.	Offers insights into the structure, functionality, and expansion of IMPaaS services.
(Wan, Waqas, Tu, Hussain, *et al.*, 2021)	Fog computing paradigm for network efficiency.	Introduces new security vulnerabilities.	Reduces latency and enhances local resource utilization.
Van Niekerk, Forcina, and Megía-Palma (2024)	Double Sarsa reinforcement learning for secure key exchanges in fog computing.	Requires significant computational resources for reinforcement learning.	Outperforms Sarsa and Q-learning in reducing false alarms and detection errors.
Illi et al.(2023)	Physical-layer security-based key generation and dynamic threshold detection for fog computing.	May require real-time adaptability for diverse network conditions.	Uses game theory and RL for enhanced attack detection.

Gupta, Patil, and Guido (2024)	Voice Impersonation (VI) dataset-based defense using QGD approach.	Limited dataset coverage for broader application.	Outperforms SVM, GMM, and BP-ANN for voice impersonation detection.
Li, Yoo, and Kettinger (2021)	Real-world voice imitation dataset for voice spoofing detection.	Requires further validation on advanced technological platforms.	First dataset from real TV broadcasts; strong mathematical modeling for speech security.
Bakare and Ekolama (2021)	Study on Man-in-the-Middle (MITM) attack threats.	Lacks implementation of defense mechanisms.	Highlights critical vulnerabilities in MITM attacks.
Aliyu et al (2021)	Cryptographic defenses (ECC, key dispersion) against MITM attacks.	Does not address new MITM attack pathways in depth.	Provides a comparative analysis of cryptographic countermeasures

2.4.1 Mobile Social Engineering Attack Case Studies

The growth of social engineering (SE) attacks in information technology remains a live threat, which calls for more effective security measures. The internet was initially designed for knowledge sharing and information exchange, with the provision of fast and free communication. But cybercriminals use these amenities to conduct identity theft and fraud, most commonly by tricking legitimate users into divulging confidential information. Phishing attacks, for example, comprise adding malicious URLs onto apparently credible links. The more online pages that are added, the more there are dangerous websites and resulting cyber threats (Vukovic and Dujlovic 2023).

Automatically detecting malicious links is proposed by Akyeşilmen and Alhosban (2024) based on a scanning and classification technique. The technique efficiently detects harmful sites even during partial page refresh or authentication. The performance evaluation of this approach in three designed applications indicates enhanced overall accuracy at 72% compared to existing approaches. Additionally, the approach improves the capacity to distinguish harmful links from legitimate ones by evaluating each hyperlink's context and significance within a website. The findings of this study can also support greater awareness among both users and website administrators, equipping them with more effective strategies to resist social engineering attacks. Knowing all types is crucial because most of web applications allow vendors and users to scan their products for malicious links. Identification of the type of threat allows it to be responded to accordingly and proper countermeasures to take. This study specifically targets three web-based platforms BuyandSell, Online Forum, and JobSearch that contain malicious links. These platforms were chosen from available research literature that tested malicious link detection systems under various scenarios.

Falade (2023) also delve into the possibility of using AI, especially ChatGPT, in conducting social engineering attacks. ChatGPT, after its introduction, has showcased great performance in diverse fields such as programming, providing specialized answers, and creating templates for text about a given topic. Coupled with its ease of use and effectiveness, these features can be harnessed to support phishing attacks or other social engineering plans within seconds. This research not only discusses SE attacks and overall preventive practices but also investigates the procedure of preparing a phishing attack through Chatbot GPT. Phishing and other types of scams come under the ambit of social engineering attacks in information security, utilizing human weaknesses to obtain confidential information, access systems without authorization, or circumvent security controls. In spite of the centuries-long history of such attacks, which go back before the emerge of computers and the internet, good countermeasures are still lacking.

Das et al.(2022) discuss security issues in the burgeoning Non-Fungible Token (NFT) space. NFTs have acquired considerable attention as investment opportunities alongside with digital collectibles, with trade volumes increasing manifold and high-

value deals taking place quite often. But security evaluation of these platforms is still minimal because most work was centered around assaults on decentralized finance (DeFi) networks and automated procedures for detecting weaknesses in smart contracts. This research is one of the first to examine security threats and market forces in the multi-billion-dollar NFT space.

de GUZMAN (2022)provides a structured overview of NFT operations, identifying three key stakeholders: users, external entities, and marketplaces. The study thoroughly examines the top eight NFT marketplaces (ranked by transaction volume) to uncover potential security risks, many of which could result in substantial financial losses. Additionally, the researchers collected a significant volume of asset and event data from NFT transactions to analyze fraudulent trading behaviors conducted under the guise of anonymity. This data also helps in understanding how external entities can manipulate NFT markets, leading to severe consequences. The dataset includes comprehensive measurements and analyses, ensuring adequate coverage of the NFT space.For instance, at the start of the data collection process, OpenSea— he largest NFT marketplace, accounting for 89.63% of assets in the dataset—had 18.2 million assets listed. The researchers successfully crawled 12.2 million assets, representing 66.94% of OpenSea's total size. Unless cross-market analysis is required, OpenSea is the primary focus, as it constitutes most of assets within the dataset. This methodology guarantees the research conclusions precisely mirror the extent of security issues involving NFTs. Summary on Mobile Social Engineering Attack Case Studies is given in Table 8.

2.4.3 Consequences of Falling Victim to Social Engineering Attacks

End users are one of the greatest weaknesses of contemporary information security systems. Social engineering — a method employed by hackers, security experts, and other attackers — is the art of manipulating people using deception to achieve unauthorized access to confidential information and secure networks. The individual attributes of people being targeted by social engineers, usually called "social engineers," have not been sufficiently studied in academic research.

To address this gap, this dissertation employs grounded theory methodology to examine discussions among both professional and non-professional social scientists. The results reveal six main characteristics of a "model victim," a theoretical person who is most vulnerable to social engineering attacks: (1) respected, (2) uneducated, (3) indifferent, (4) sociable, (5) well-connected, and (6) confident. Furthermore, heuristic categories such as sociodemographic characteristics, social roles, and organizational roles are examined as determinants of decisions regarding a target's vulnerability. Implications for ethical concerns, future studies, and policy-making are also addressed in the study.

Bullée and Junger (2020)examine social engineering as a common phenomenon of cybercrime and assess several interventions aimed at minimizing vulnerability to these attacks. Their analysis explores if particular undertakings may diminish vulnerability toward manipulation. It scrutinizes the efficacy and composition of strong treatments too. The study, performed using an experimental method, tested at least one approach to minimizing susceptibility to social engineering. The Scopus database was searched for studies relevant to the topic. The traits which social engineers find in prospective victims. Research into fraud victimization is of related interest, and researchers often have been concerned with three sets of attributes: sociodemographic, personality, and lifestyle. Age is typically argued among sociodemographic factors since some research implies that elderly persons are more prone to scams, a finding to which both popular culture and law enforcement communities are sympathetic

Based on a total sample size of 23,146 individuals, the authors reviewed 19 studies, yielding 37 effect sizes. They analyzed the available training programs, intervention strategies, and their effectiveness. Data on intervention settings, characteristics, and study methodologies were collected, with heterogeneity assessed through random-effects models. The findings reveal notable differences in how effective various interventions are. While some measures proved entirely ineffective, others were highly successful. High-intensity interventions were found to be more effective than low-intensity ones, and targeted interventions yielded better outcomes than generalized approaches.

Skivington et al. (2021) concludes that the effectiveness of intervention strategies varies significantly, allowing practitioners to refine awareness programs for better impact. According to the authors, this research represents the first comprehensive comparison of social engineering countermeasures. While some interventions were straightforward, others were complex. It is reasonable to assume that more intensive interventions produce stronger long-term effects. However, such interventions may also require greater time, effort, and financial resources. As a result, a simple yet efficient approach is often the most cost-effective solution.

Quach et al(2022) discuss how the rise of social media and advancements in digital technology have facilitated communication while simultaneously increasing the risk of private information being exploited. Social engineering has emerged as a method used by malicious actors to gather sensitive personal information, compromising the victim's privacy and causing potential harm. One of the most prevalent and dangerous threats individuals face is phishing through social engineering. The research also outlines survey-based techniques employed to counter such attacks, create public awareness, and recover people from phishing scams.

Phishing is most often composed of spurious mails or viruses disguising themselves as authentic sites and lead people into divulging secret information like account numbers, log-in names, and passwords. For instance, an attacker may send an alert or mail message saying that a prize has been won by the victim and then he or she needs to access a link if he or she wants to be awarded it. The fraud guides the target to a nonexistent webpage, and there the individual has to give certain details concerning the self, which includes telephone numbers and banking information. The attacker exploits such an item of information after acquiring it for identity or money theft using social engineering techniques.

To combat social engineering attacks, the research suggests some prevention measures and solutions. Since the attacks are founded on human trust, there will need to be effective countermeasures focused on awareness, education, and technology defense against phishing and other social engineering tactics. Summary of Key Studies on Social Engineering Interventions is given in Tablr 9.

2.5 Financial, Privacy, and Security Risks Associated with These Attacks

Blockchain technology, designed for the digital era, fascinates the present generation to a higher degree. The Internet of Things (IoT) also stands to gain a lot by being combined with blockchain technology. Global adoption of IoT technology across various industries has enhanced the growth of distributed systems to a large extent. Blockchain's decentralized system for data management offers secure storage of data and transactional dispersal over networks.

Mishra (2023) examines recent defense methods in case of cyber attacks and presents a complete review of blockchain security surroundings. The study reviews the basic concepts behind blockchain, its potential vulnerabilities, and its safety risks and showcases how these kind of issues are capable of being circumvented .Additionally, this study reviews strategies to enhance security within blockchain and provides extensive detailed explanations about pertinent concepts applicable for use in most blockchain systems.It also provides security solutions to counter threats, pointing out the open problems and possible research areas for enhancing blockchain-IoT integration.

Security is the top priority with the evolution of blockchain technology, especially in terms of decentralization, immutability, anonymity, and auditability.This research presents current analysis of blockchain parameters and vulnerabilities in digital-physical systems. It also explains contemporary security solutions and practical uses of blockchain technology to counter security threats. With the growing interest from academics and industries alike, this research analyzes current security solutions for blockchain across different applications and suggests viable approaches to solving security vulnerabilities. Moreover, it enumerates open challenges, unresolved research needs, and overlooked requirements that can improve blockchain-IoT performance

Singh, Hosen, and Yoon (2021)provides detailed analysis of FinTech financial, privacy, and security risks, with valuable contributions to future researchers and practitioners. The study categorizes FinTech cybersecurity threats, detection techniques, and countermeasures into a unified taxonomy. The study, in investigating recent

developments in FinTech security, aims to raise awareness and bridge gaps hindering seamless technology integration. Furthermore, it provides a summary of security and privacy challenges in the financial sector and recommends frameworks to improve cybersecurity in bank networks. The study emphasizes the critical role of cybersecurity in FinTech and examines its impact on online financial services.

Yaacoub et al. (2022) identify the increasing employment of robotics in industries, for example, in logistics, medical care, manufacture, the army, and policing. Robotics seeks to improve efficacy and enhance life. Robust security threats and cyberattacks upon robotic systems constitute a key cost and operational danger. Unforeseen failure exists, but nasty cyber attacks impose complex threats like unauthorized robot management and control used to cause humongous financial damage.

Botta et al. (2023)examines the most important security vulnerabilities, threats, and risks to robots and the most common robot security attacks. To enhance the security of robots, the study suggests an advanced set of countermeasures that involves multi-factor cryptography approaches and robust device and user authentication protocols. The research also elaborates on emerging robot security innovations and examines their suitability across various sectors, including construction, agriculture, the military, disaster recovery, and healthcare.

The study provides detailed analysis of FinTech financial, privacy, and security risks, with valuable contributions to future researchers and practitioners. The study categorizes FinTech cybersecurity threats, detection techniques, and countermeasures into a unified taxonomy. The study, in investigating recent developments in FinTech security, aims to raise awareness and bridge gaps hindering seamless technology integration. Furthermore, it provides a summary of security and privacy challenges in the financial sector and recommends frameworks to improve cybersecurity in bank networks. The study emphasizes the importance of cybersecurity in FinTech and examines its impact on online financial services.

C. Wang et al (2021)identify the increasing employment of robotics in industries, for example, in logistics, medical care, manufacture, the army, and policing. Robotics seeks

to improve efficacy and enhance life. Robust security threats and cyberattacks upon robotic systems constitute a key cost and operational danger. Unforeseen failure exists, but nasty cyber attacks impose complex threats like unauthorized robot management and control used to cause humongous financial damage.This research examines the most important security vulnerabilities, threats, and risks to robots and the most common robot security attacks. To enhance the security of robots, the study suggests an advanced set of countermeasures that involves multi-factor cryptography approaches and robust device and user authentication protocols. The research also elaborates on emerging robot security innovations and examines their suitability across various sectors, including construction, agriculture, the military, disaster recovery, and healthcare.

The investigated studies provide concrete insights into economic, privacy, and security risks with blockchain, FinTech, and robotics and highlight key weaknesses and suggest mitigations. Security of blockchain is elaborated deeply but without experimental validation, making its practical utilization restricted. Threats to cybersecurity with FinTech are categorized under an extended taxonomy but are based on real hazards without sufficient experimentation. Similarly, robotic security studies point out major threats without any talk of field implementation. Cryptographic models suggested are purely theoretical solutions with no real-world implementation. While these papers make a substantial contribution to the insight of cybersecurity threats, their reliance upon theoretical models rather than empirical validation underscores the need for further experimental research.

Research Gap

The fast growth of India's telecommunication sector, studies on cybersecurity in the sector have largely concentrated on technical weaknesses like malware, encryption, and intrusion detection systems. A substantial knowledge deficit persists about the human element within security breaches, especially social engineering attacks (SEAs). Existing studies largely overlook the mechanism through which attackers employ psychological manipulation techniques—such as phishing, vishing, and smishing—to deceive telecom customers and customer care representatives. Security improves with regulatory

standards besides technological advancements. However, social engineering attacks (SEAs) endure, revealing current measures such as multi-factor authentication as well as fraud detection systems do not adequately counter threats rooted in human behavior. Further, research on SEAs in India's telecommunication sector is limited too, and most of it has been carried out on banking or corporate security, without paying heed to an acute examination of the targeted vulnerabilities inherent in telecom customer service procedures.

In addition, evolving threats fueled by artificial intelligence (AI) and automation further enhance the research void. AI-phishing emails, deepfake voice calls, and synthetic identity theft are new dangers that current security paradigms are not ready to counter. Current research is not able to explain how SEAs fueled by AI can be countered in India's telecom ecosystems, especially during customer support processes where attackers use impersonation tactics to obtain unauthorized access. Furthermore, there is limited empirical research that quantifies the incidence and economic burden of SEAs in Indian telecom companies, hindering the framing of focused mitigation strategies. Future studies need to fill these gaps by incorporating behavioral science into models of cybersecurity, augmenting real-time AI-based threat detection, and implementing comprehensive training programs for telecom staff and customers to combat social engineering threats.

Social engineering attacks (SEAs) are one of the highest-order cyber threats that are founded on exploiting human psychology instead of on technological weaknesses. While conventional cybersecurity controls like firewalls, encryption, and intrusion detection systems respond to technological attacks, social engineering evades them by misleading people into sharing confidential information. Among these different types of SEAs, others have been found to be discovered through research, including phishing, spear-phishing, vishing, smishing, impersonation scams, and reverse social engineering. These types of attacks are overwhelmingly in the booming telecommunications sector in India, where customer care business and mobile networks offer great prospects for hackers to attack.

The study highlights the use of psychological manipulation in SEAs, calling attention to the way deadlines, trust, and authority are being exploited by attackers in misleading others. The study revealed that even experienced individuals and organizations can be deceived, highlighting the need for awareness campaigns and training initiatives. However, the effectiveness of educational interventions varies due to the evolving tactics employed by attackers. AI-driven phishing, deepfake voice calls, and synthetic identity theft are new threats that are difficult to fight for conventional security solutions.

The review also explores countermeasures, including machine learning-based phishing detection, reinforcement learning for secure key exchanges, and cryptographic defenses against impersonation and Man-in-the-Middle (MITM) attacks. However, many proposed solutions remain theoretical, with limited empirical validation and real-world implementation. Research in blockchain, FinTech, and robotic security highlights critical vulnerabilities but lacks experimental testing, leaving gaps in practical cybersecurity solutions.

Despite the increasing regulatory standards and security enhancements, existing frameworks remain insufficient to mitigate SEAs effectively. There is a notable research gap in studying SEAs within India's telecom sector, particularly regarding the economic impact and real-time threat detection. Future studies should integrate behavioral science with AI-based threat detection and focus on empirical research to quantify SEAs' risks and develop robust defense mechanisms. Strengthening customer awareness, improving telecom personnel training, and deploying advanced AI-driven security frameworks will be crucial to combating evolving social engineering threats.

This also discusses countermeasures such as machine learning-based phishing, reinforcement learning for secure key exchange, and cryptographic protection against impersonation and Man-in-the-Middle (MITM) attacks. Most solutions are still theoretical with little empirical support and implementation in the real world. Blockchain, FinTech, and robotic security research point out important weaknesses but do not test them experimentally, therefore practical cybersecurity solutions remain incomplete.

Despite the growing security standards and safety measures, present frameworks are lacking to counter SEAs effectively. There is immense research lacuna in examining SEAs in the telecom industry in India, more so in respect of the economic effect and near-real-time detection of threats. Future research can combine behavioral science with AI threat detection and pursue empirical research in order to provide quantifiable analysis of SEAs' risks and build effective defense mechanisms. Enhancing customer education, enhancing telecom staff training, and implementing sophisticated AI-based security systems will be essential in fighting emerging social engineering attacks.

Chapter 3

Research Framework

This chapter details the research framework, including the conceptual model, hypotheses, and methodological strategy, used to investigate social engineering attacks on customer support units of mobile service providers in Mumbai. The research aims to identify attacker approaches, weaknesses in customer support processes, and the effectiveness of countermeasures.

The conceptual model illustrates the interaction between key factors such as employee awareness, security measures, organizational policies, and attack methodologies. Drawing from existing literature and industry analyses, the hypotheses explore how these factors affect the probability and impact of social engineering threats. The study utilizes a mixed-methods design, integrating both qualitative and quantitative methods to achieve a thorough comprehension of the issue. Data is collected through surveys, interviews, and case study analysis, with a focus on customer support personnel and security professionals in Mumbai's mobile service provider industry. Ethical aspects are taken into account to guarantee the protection of data privacy and uphold the integrity of the research. Data analysis involves statistical and machine learning methods to identify patterns and relationships, alongside with descriptive thematic analysis to understand employee behavior and responses to social engineering attempts. This multifaceted approach ensures a thorough evaluation of the issue, leading to informed recommendations for enhancing cybersecurity measures.

3.2 Conceptual Framework

The conceptual framework categorizes the key elements influencing social engineering attacks into three primary domains: human factors, organizational variables, and attacker strategies. Human factors encompass employee awareness, training, and susceptibility to psychological manipulation (Saleem *et al.*, 2024). Organizational

variables include security policies, authentication processes, and incident response mechanisms. Attacker strategies focus on techniques of elicitation, exploitation, and deception. These categories facilitate an analysis of social engineering attack dynamics and the identification of areas for security improvement within mobile service provider customer support departments.

As detailed in Chapter 1, social engineering attacks encompass various methods. This framework focuses on four key types—phishing, pretexting, baiting, and impersonation—to analyze their specific impact on mobile service providers' customer support.

While Chapter 1 provided comprehensive definitions of these attack types, this section outlines how these categories are applied within the research framework to structure data collection and analysis

Chapter 1 described the roles of customer service representatives, account assistants, and technical support personnel. Here, these roles are considered to assess their varying levels of vulnerability to social engineering within the mobile service environment

This study investigates the targeted information—personal customer details, account credentials, and billing information—to understand the potential consequences of social engineering attacks, building upon the definitions established in Chapter 1.

Chapter 1 discussed various security measures employed to counter social engineering. This section of the framework outlines how the effectiveness of these measures is evaluated within the research design

The framework assesses the impact of security protocols, employee training, and incident reporting mechanisms on the frequency and success of social engineering attacks, considering the detailed explanations of these measures provided in Chapter 1.

Figure 3.1 illustrates the four types of social engineering attacks we considered in this study, which helped us categorize the attack types reported by participants.

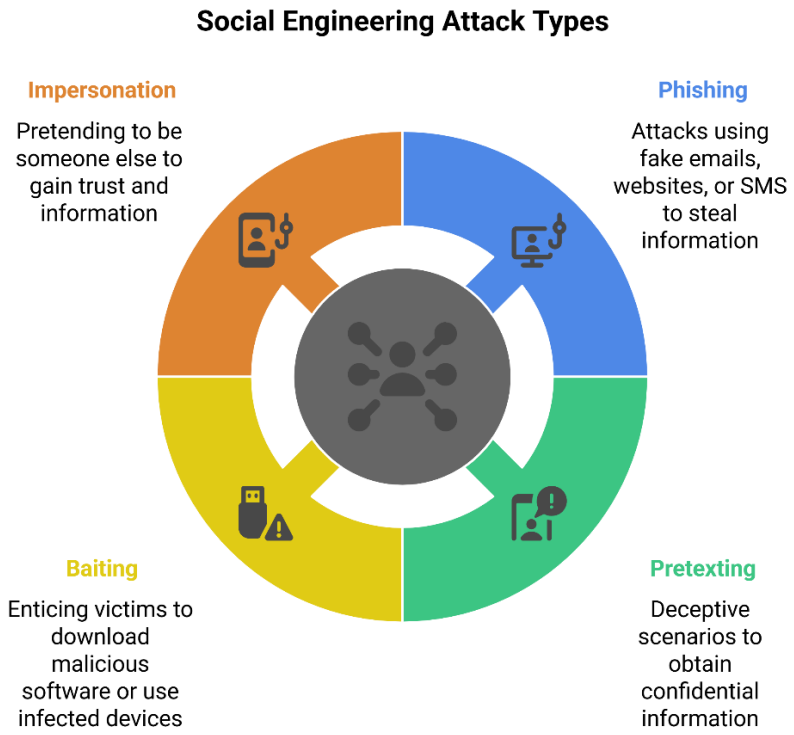

Figure 3. 1: Social Engineering Attack Types

Figure 3.2 shows the employee roles and data access points we investigated to understand which roles might be most vulnerable.

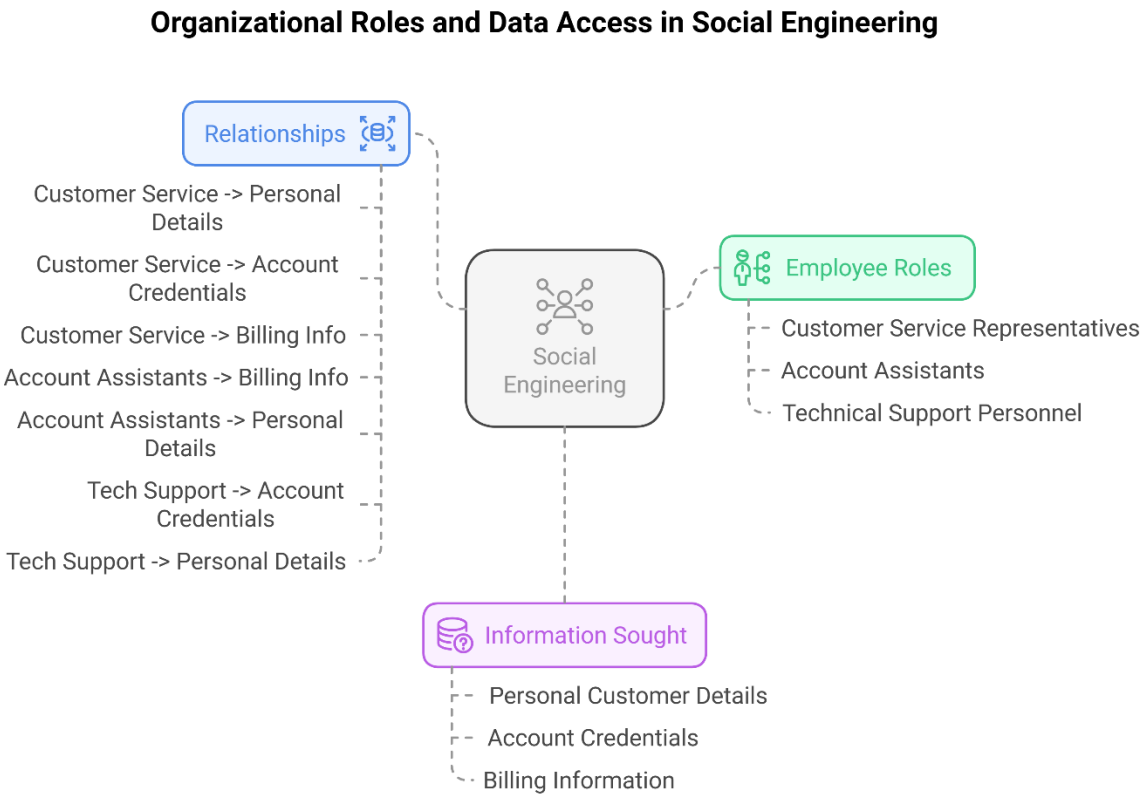

Figure 3. 2: Organizational Roles and Data Access in Social Engineering

Figure 3.3 illustrates the categorization of information targeted by social engineering attackers in this research. Knowledge of these categories is crucial for analyzing the impact of such attacks and developing effective countermeasures (Rains, 2020b).

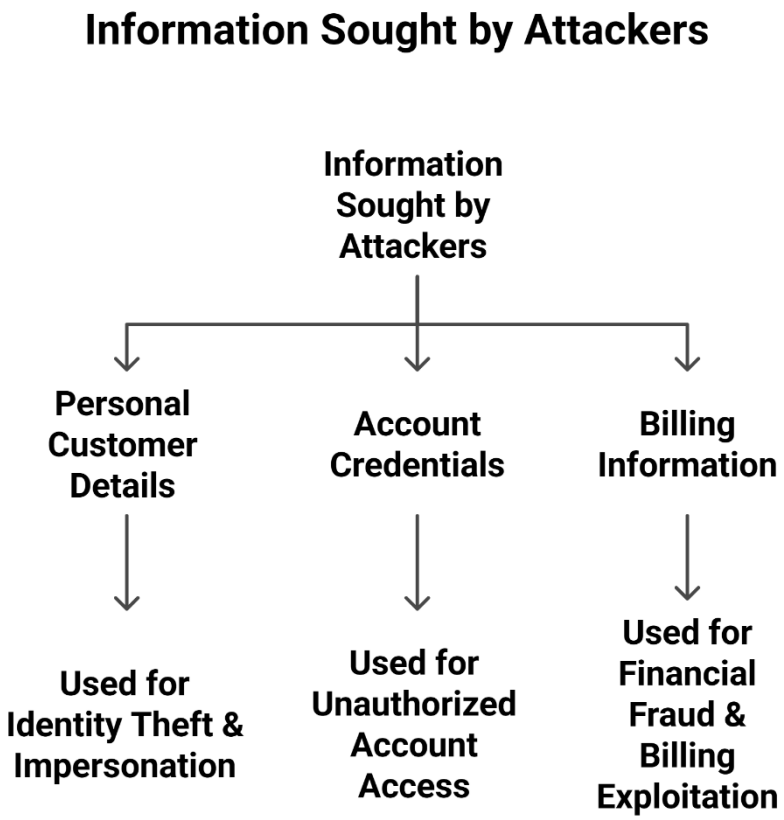

Figure 3. 3: Information Sought by Attackers

3.3 Research Design

This investigation uses a measurable study approach. The study precisely analyzes social engineering intrusions directed toward customer assistance staff among Mumbai's cellular network corporations since it employs questionnaire statistics. The research design relies on systematic collection of data and statistical analysis for meaningful deductions relating to patterns in attacks, targeted job roles of the employees, and the efficacy of implemented security measures. The survey was conducted for determining:

3.3.1 Demographic and Job Role Information

Gathering demographic and job role information from customer support teams at mobile service providers is crucial to assess their susceptibility to social engineering attacks. Workers of different roles such as account assistance, technical support, and billing frequently interact with customers and handle confidential data, including personal information, account credentials, and billing details. Work experience between employees varies; being their limited familiarity with the safety protocol can be more easily manipulated, while experienced employees can be decent over time. The degree of customer engagement additionally has a vital part in susceptibility to potential incursions. People contending with an abundance of client inquiries daily are predisposed to encounter deceptive practices consequently. Recognizing these factors is vital for designing effective security training programs and implementing control measures to enhance protection against social engineering threats (Yue *et al.*, 2021).

3.3.2 Social Engineering Attack Encounters

Social engineering threats encountered by customer support teams in mobile service providers often include phishing, pretexting, baiting, and copying, all of which take advantage of the human trust to get sensitive information. Employees usually report phishing emails and messages, which mimic official communication, while pretending the attacks are usually attackers that pretend to be employees or officers to ignore the security protocol to employees. However, like a USB drive containing a fake propaganda offer or malware, the batting strategy is less frequent; they still present a risk. Particularly on the phone's copy of the phone, SIM swaps are common in fraud cases. The occurrence of these attacks varies, with some employees experiencing many attempts each week, especially in situations with important customer interactions. Attackers often use urgent requests, emotional manipulation, and technical jargon to build trust and extract information. Employees feel that the complexity of such attacks is increasing, with some frauds looking highly authentic, but the success of such efforts primarily depends on people's awareness and the efficacy of security training sessions.

3.4 Research Hypotheses

The following hypotheses were formulated to address the research questions outlined in Chapter 1.important weaknesses and suggest specific safety reforms. In line with the study's goals and previous research, the following hypotheses have been established:

Each hypothesis directly corresponds to one of the aims of the dissertation. For instance, H1 and H2 are designed to examine factors relevant to Objective 2

Objective 1: Identifying Common Social Engineering Attacks

Regarding former studies, the employee function plays a critical role in determining the essence of the social engineering attack experienced since various job functions put individuals at various risk levels. Research has indicated that customer service representatives, technical support personnel, and billing clerks are the most vulnerable to phishing, pretexting, impersonation, and baiting attacks because they have access to confidential customer data. For instance, phishing tends to target billing clerks with massive email traffic, pretexting and impersonation affect customer service representatives dealing with account changes and authentications. Furthermore, baiting attacks against technical support staff were found in existing research through infested USB keys or pirated software downloads by virtue of them being part of IT maintenance work. Empirical data also confirms such patterns, and it shows how social engineers devise attack plans to fit an employee's role at work, making use of tactics of urgency, authority, and trust. The following hypothesis is thus formed:

- H_0: Social engineering attack type is not greatly related to employee roles. For employees, it is not that they encounter a specific attack type because of the roles they have.
- H_1: Employee roles relate greatly with the social engineering attack type encountered by employees.

Objective 2: Identifying Targeted Employee Roles & Information Sought

Studies indicate that social engineering attacks usually target specific individuals in an organization since the attackers select employees with direct access to sensitive information or system control. Customer support representatives, account assistants,

and technical support workers are particularly vulnerable due to their constant dealings with customer accounts, authentication mechanisms, and sensitive data. Evidence indicates that attackers often attack customer support staff by posing as troubled customers or top executives, tricking employees into skipping verification processes. In addition, research has shown that billing and account management staff are frequently targeted for phishing and baiting attacks, because they deal with financial information and payment details. Empirical findings identify technical support personnel to be easily deceived into undertaking unauthorized password reset or malicious code installations and therefore become most susceptible to social engineering attacks. Further, social engineers tailor their assaults depending on profession using psychological manipulations such as the sense of urgency, familiarity, and authority in order to procure compliance. These findings emphasize that some employee positions are at higher risk, thus giving rise to the following hypothesis:

- H_0: There is no significant association between employee roles and the likelihood of being targeted in social engineering attacks.
- H_1: Certain employee roles are significantly more predisposed to be targeted in social engineering attacks.

Objective 3: Assessing Security Measures

Research has continuously shown that implementing strong safety procedures can greatly reduce the success rate of social engineering attacks by improving employee awareness and improving methods of detection. Multi-factor authentication (MFA), strict access control, and employee training programs such as safety measures, pretexting, batting, and impressing attacks serve as significant defences. Studies suggest that organizations with fully security awareness training are seen as the efforts of low social engineering, as employees become more efficient at identifying and responding to misleading. In addition, event reporting mechanisms are necessary in reducing the frequency of the attacks, as trained employees can help prevent these incidents from growing. Research also indicates that companies face high rates of successful social engineering attacks without well-defined security protocols, as the attackers take advantage of informal staff and weak authentication procedures to have unauthorised

access. Additionally, studies on safety compliance behaviour suggest that implementing strict adherence to procedures can significantly reduce the risks of the attack, as employees follow the installed guidelines when confirming the customer's identity and managing sensitive information. Given these empirical findings, it is clear that the implementation of security measures directly affects the frequency and success rate of social engineering attacks, which creates the following hypothesis:

- H_0: There is no significant relationship between the security measures in place and the frequency of social engineering attempts.
- H_1: The presence of security procedures significantly reduces social engineering attacks.

3.5 Data Collection Methods

Research employed a quantitative research method to widely analyse social engineering attacks on customer support employees in mobile service providers. A structured questionnaire was used as the main tool for data gathering, allowing the researchers to obtain uniform responses from employees in different roles. This method ensured consistency by facilitating comparative analyses of factors such as attack frequency, targeted job positions, and the efficacy of security protocols. To maximize accessibility and boost participation rates, the survey was spread through online and offline channels. Participants were guaranteed confidentiality to promote honest reporting of any social engineering incidents they had experienced. before the full distribution, the questions were improved for lucidity and pertinence using a preliminary assessment with few workers. Information gathering lasted four weeks as diverse mobile service vendors within Mumbai engaged in research.

3.4.1 Survey Instrument

A delineated questionnaire functioned in the capacity of the primary data accumulation mechanism. It included items that were both closed-ended and Likert-scale. Every segment, distinctly partitioned, was created for capturing key aspects concerning security practices coupled with social engineering threats. The preliminary segment

requested demographic information. It included job designations, spans of experience, and the regularity of communication. The ensuing segment dwelled on personnel encounters with social engineering incursions since it chronicled the varieties faced, including phishing, pretexting, baiting, and impersonation, the stratagems adopted by perpetrators, and workforce sentiments concerning the intricacy of such menaces. A further section evaluated security measures by examining employee awareness, the effectiveness of training programs, and adherence to organizational security policies. The final section explored incident reporting procedures and how organizations respond to social engineering threats. The survey was created to ensure both validity and reliability, using questions informed by previous research and insights from cybersecurity experts.

3.4.2 Sample Size

The study gathered 60 responses from customer support employees in various roles at mobile service providers in Mumbai. This included customer service representatives, account assistants, billing support staff, and technical support personnel, which ensured a wide range of perspectives on social engineering threats. A purposive sampling method was employed to specifically target employees who frequently engage with customers and handle sensitive account information, as they are especially sensitive to social engineering attacks. The preliminary assessment necessitated a sample dimension of 60. The investigation offered perceptions into assault patterns, staff cognizance, and the effectiveness of current safety procedures. Taking the sample across diverse firms augmented the conclusions' applicability inside the mobile service provider sector.

3.4.3 Variables Measured:

In the research, variables were categorized into dependent variables (DVs) and independent variables (IVs) to analyse the impact of employee roles and security measures on the likelihood of social engineering attacks.

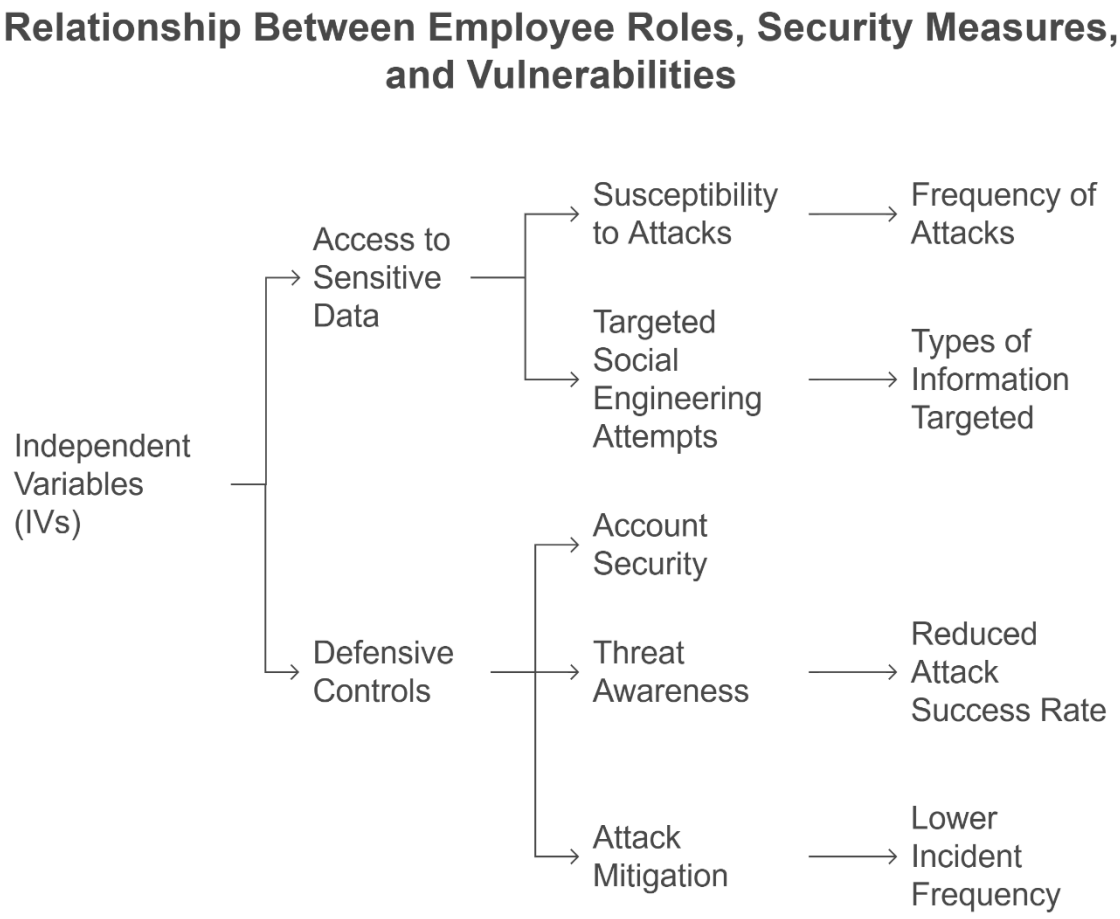

Figure 3. 4: Independent Variable Measure

Figure 3.4 visually illustrates the intricate relationships among employee roles, security controls, and vulnerabilities, demonstrating how access to sensitive information and protective measures collectively shape an organization's security landscape. At the center of the diagram lie the independent variables and security controls, both of which play a crucial role in influencing the likelihood of social engineering attacks. Staff with greater access to sensitive information—customer data, account details, and finances—are more at risk for phishing, pretexting, and impersonation attacks. The diagram shows sensitive data at a high risk for worker-customer data, account details, and finance: phishing, pretexting, and copy attacks. High risk means high frequency of attacks, which determines what kind of information the hackers exploit. The diagram also highlights the crucial role of defensive controls, such as multi-factor authentication (MFA), employee

safety training, and event reporting, which reduces the risk. Effective account security protocols together with anticipatory threat awareness initiatives function together to lower the rate of successful social engineering breaches, which results in a reduced number of security incidents. How the relationship is shown via the digestive purpose of the diagram indicates that active safety control, rule-based access control, together with frequent training, for example, can be greatly lessened to diminish the company's risk. Strain over education, policy implementation, and oversight is present. That variable's oscillation underscores why we require safeguards. This model may be applied as a strategic tool for risk determination, which helps companies implement strong cyber defence mechanisms to create custom safety policies, increase vigilance, and protect them from constant hazards.

Independent Variables (IVs)

a) Employee Role

A worker executing a role within the Customer Assistance Department ascertains their susceptibility toward social engineering attacks, as they connect various job titles to differing quantities of access to sensitive customer data. Employees in account support, technical assistance, and billing services frequently handle sensitive information such as customer account details, billing records, certification data, and service modifications. These employees are typically authorized to reset passwords, change account settings, and grant or withdraw access, so they can become a high-value goal for cybercriminals who are engaged in social engineering to help them take unauthorised action. Attempts to try to misuse the control and access permissions of the employees, which also do to control accounts, steal personal or financial information, or even disable safety controls.

The study objective concerning data revelation and access privileges is for determining if social engineering exploits unevenly single out staff within particular vocations. That inquiry was designed for ascertaining if assailants concentrate upon specific employment designations which can access patron information to a greater extent, or whether social subterfuge incurs randomly throughout each occupation sustaining clientele. The recognition of these attack patterns is important in increasing security

policies, increasing role-oriented training and limiting unwanted access to sensitive information. Whenever specialists connect labor positions to attack frequencies, they formulate specified protective procedures. This confirms each job function is strengthened by suitable cybersecurity cognizance. It further enables each employment role to skillfully diminish manipulation based menaces.

b) Security Measures in Place

Employees require appropriate instruction to confront social engineering risks since strong protective systems furnish the principal safeguard. Investigators examined the security protocols including MFA and employee training programs, event reporting functions. These techniques aid in precluding occurrences alongside with achievements of social engineering attacks. As a security protocol MFA compels employees to validate their identity through sequential authentication procedures which link passwords to time-sensitive verification codes or biological confirmation methods. The additional security feature creates a strong barrier which prevents unauthorized access to sensitive customer data during credential theft.

An organization's security framework relies significantly on employee training as a core element. Since staff act as the initial barrier against phishing, vishing, and pretexting attacks, they must be educated to recognize and comprehend the tactics used by attackers who exploit human behavior. The research examined not only the presence of comprehensive cybersecurity awareness initiatives but also the level to which workers adhere to the implemented policies. The study investigated training programs regarding their coverage of phishing email identification and customer identity authentication together with secure information processing protocols in addition to training frequency. The assessment of event reporting processes focused on employee ability to detect suspicious activities and their successful recording and reporting of such findings. Real-time reporting of potential security risks through an established reporting culture allows organizations to start proactive measures that prevent successful attacks. The study evaluated the existence of non-punitive reporting systems that protected employees who reported suspicious activity.

The study evaluated organizational readiness along with employee responsiveness through an analysis of security procedures. Understanding how strong existing cybersecurity policies are besides employee compliance levels provides organizations with critical information about necessary improvements which will lead to more effective security frameworks and stringent compliance policies along with specific employee training on identifying social engineering threats.

Dependent Variables (DVs)

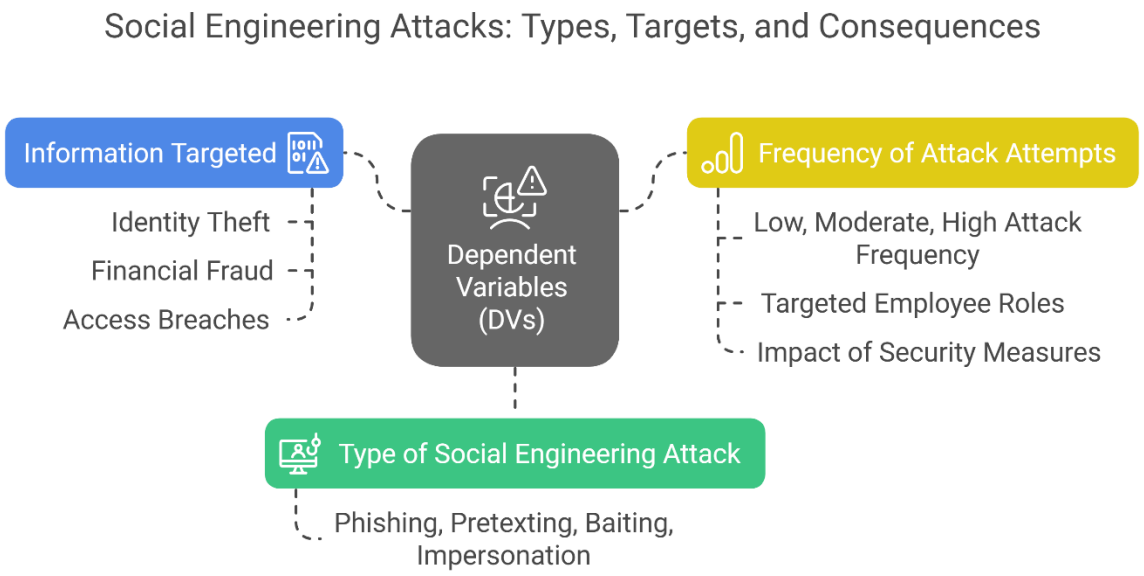

Figure 3. 5: Dependent Variable Measure

Figure 3.5 maps the interrelation between social engineering attacks, types, objectives, and impacts, explaining how these variables interact under an organizational security context. The centre of the figure has variables (DVs) dependent on which is determined by three major components: targeted information, frequency of attack efforts, and categories of social engineering attacks. Targeted information includes identity theft, financial fraud, and access breaches, which represent the main goals of the attackers when targeting employees. The frequency of attack efforts is at least more unsafe with targeted positions such as technical support, account management, and billing services, while the effectiveness of the security mechanism determines the overall vulnerability of an organization. Social engineering attack types include phishing,

pretexting, baiting, and impressing; all are used to release sensitive information or provide unauthorised access to employees using deception strategies in different forms. The diagram indicates the interrelation of these factors, indicating that some attack vectors result in specific safety threats and organizational risks. By realizing these relationships, the organizations are able to successfully create specific safety policies, role-specific training programs and safety measures to combat the risks incurred by social engineering attacks.

3.5 Research Design

A theoretical research design with mixed approaches combines qualitative and quantitative methods within a coherent theoretical framework to investigate complex research problems comprehensively. The integration of diverse perspectives and methods, this approach enables researchers to develop an knowledge of the researched facts, contributing to theory development and practical applications in the field. The Mixed method research design is presented in Figure 3.6.

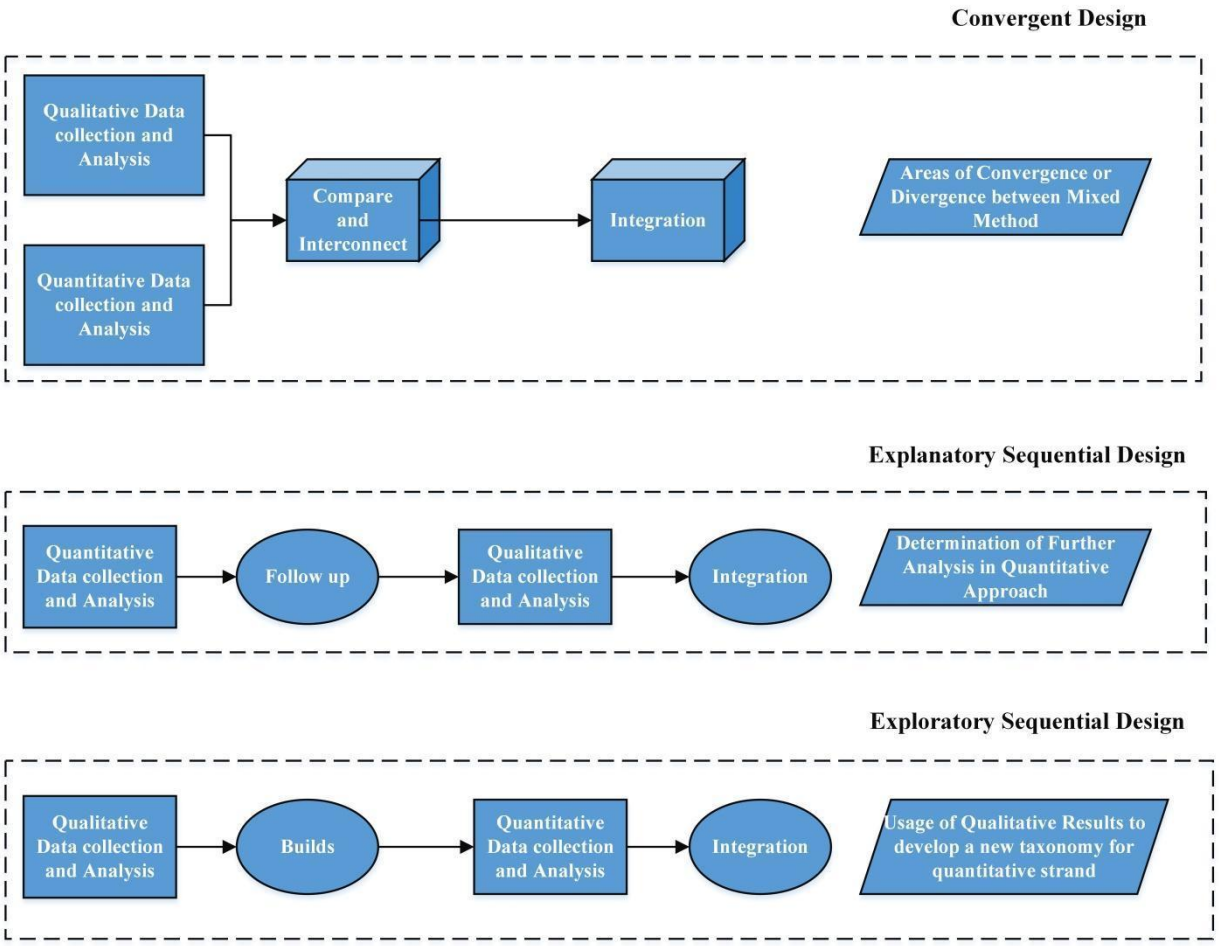

Figure 3. 6: Research Design for Qualitative and Quantitative Approach in Social Engineering Attack

3.5.1 Theoretical Framework

A theoretical framework constitutes the groundwork of study design as the selection of research methods denotes the collection of the information and analysis approach. Incorporating diverse theoretical approaches employed for the investigated question within the framework necessitates a mixed-method theoretical research design. A demonstration is a probe into the influence of technology upon psychological wellness for the reason that it uses socio psychological tenets, interface ideas, and wellness conduct principles. The study is improved in both depth alongside with width by uniting a range of different theoretical approaches together. It permits expanded concepts about the problem under study.

3.5.2 Qualitative Component

The qualitative component of research design pertains to information refined and thorough, securing subtlety and affluence to apprehend the research question. This method permits researchers to scrutinize the participants' accounts, experiences, and tasks within their environment. Under a theoretical research paradigm, qualitative data provides rich information about subjective meaning processes that form the phenomenon of study. For instance, in study on adopting renewable energy technologies, qualitative interviews can identify motivations, values, and challenges that affect people's decision-making, meet the obstacles for a rich understanding, or adopt drivers.

3.5.3 Quantitative Component

For ascertaining variables and assessing conjectures, quantitative aspects within research design seek to garner numerical facts cultivated inside a theoretical framework. This function employs techniques such as surveys, experiments, in addition to quantitative analysis of the available dataset to systematically gather and scrutinize data. The quantitative approach undertakes an organized with purposeful inquiry of the

research issue. It acts via scrutiny of tendencies, connections, and links among those variables. In a theoretical research paradigm, quantitative data is used as empirical proof for confirmation or contradiction of theoretical suppression. For instance, in a research project measuring the effectiveness of educational intervention on educational performance, the quantitative questionnaire can follow the test scores of the students before and after intervention, providing the average data on its effects.

3.5.4 Integration of Data

A fusion of qualitative along with quantitative information is an intrinsic aspect of a theoretical research design that integrates methods artfully. Investigators integrate knowledge originating from qualitative and quantitative origins through methodologies like triangulation, complementation, and amplification; this furnishes a thorough comprehension of the studied subject. Data gets gathered through varied methods for comparison via the triangle. This assessment may validate or corroborate outcomes, augmenting the investigation's dependability. The supplement takes advantage of both qualitative and quantitative data to introduce various insights on the same phenomenon, so a richer interpretation. The expansion is realised when one form of data is employed to expand or expand on the results obtained from another, deepening the general analysis. Since this research integrates diverse evidence sources, it strengthens the validity, reliability, and robustness of the design study's findings so results are strong and rich.

3.6 Data Collection Procedures

Current research uses a mixed-methods approach for scrutinizing social engineering intrusions aimed at customer support teams among cellular network suppliers located in Mumbai using integrated qualitative with quantitative data acquisition including interpretation. Research approaches include diverse strategies, since they incorporate prior incidents and interview customer support agents and security staff in person so they may acquire qualitative information regarding past challenges. In addition, the customer surveys were conducted within those who were victims of social engineering attacks, also the surveys gathered quantitative information on the frequency of the attack, the methods of attack, plus their general impact. As additional evidence, the study of a case of social engineering attacks against mobile

service providers was investigated. For recognition of overarching topics and trends, thematic scrutiny in data interpretation concerning interview replies was used regarding worker perspectives plus safety matters. Answers from the survey were scrutinized, demographic patterns were appraised, and attacks including their effects were gauged through statistical methods used concurrently. The study's discoveries stood in contrast to case studies alongside preceding publications. The analysis scrutinized by pinpointing the assault's configuration's principal similarities with disparities. These outcomes prompted proposals, so mobile providers may strengthen security protocols throughout Mumbai. Reinforcing security protocols strengthens their skill to efficiently oppose social engineering attacks.

Basit et al.'s (2021) investigation contemplates aspects regarding communicative conduits throughout a phishing intrusion, targeted devices, attacking ways, and defense strategies. Perpetrators employ various modes of communicating to deceive victims via phishing, wherein human contact functions as the key means of assault. Earlier scholarship referenced seven discrete avenues for correspondence within phishing schemes. Transgressors capitalize on voice over internet protocol VoIP. Email likewise is used via perpetrators, as well as instant messaging applications, blogs and forums, websites, online social networking sites, and mobile platforms. As phishing takes advantage of connectivity online, the gadgets victims are using are essential in an attacker's plan. Phishing can happen on smart devices, voice-enabled assistants, computers, and wireless-enabled devices like those running using VoIP and cellular networks. Choosing between attacking modalities may primarily depend on device type and channel of communication, underlining how technological weaknesses become key in foiling phishing exploits.

This study investigates the four basic building blocks of a phishing attack, which are the communication channels, target devices, attack techniques, and countermeasures. Phishing mainly deals with human interaction using different communications media, where the human victim is the core target of attacks. Previous literature has identified seven most important communication channels used to launch phishing attacks, which consist of voice over internet protocol (VoIP), email, message platforms, blogs and forums, websites, social networks online, and mobile applications.

Phishing is dependent on online connectivity, and therefore the tools employed by victims largely determine the plan of attack. Phishers can exploit smart devices, voice-enabled technologies, desktop computers, and Wi-Fi-connected smart devices, including those accessed over VoIP and mobile networks. One can establish efficient security mechanisms via comprehension of communication platforms, device vulnerabilities, together with phishing methods. These instruments remain important for combating such menaces.

Attack techniques fall into two primary categories: attack launch methods and information gathering mechanisms. Several techniques are employed in launching an attack, such as malicious attachments, email spoofing, social engineering trickery, URL and web site spoofing, smart voice response exploitation, reverse social engineering, spear phishing, man-in-the-middle, fake mobile internet browsers, and embedded malicious web content. Besides initiating the attack, cybercriminals use diverse data collection techniques as they amass information prior to, during, following a victim's interaction with the attack. These techniques fall within two categories: automated methods, including keyloggers, recorded messages, and spoofed websites, and manual methods, which include social networking trickery and psychological manipulation. To counter these threats, proactive and reactive countermeasures are put in place to intercept, block, and render attacks ineffective at different stages, minimizing the abuse of compromised data. These measures go a long way towards detecting and halting cyber threats, protecting users from phishing and social engineering attacks. Countermeasure methods of phishing attack detection are divided into four major approaches: (1) Machine learning methods, (2) Deep learning-based methods, (3) Scenario-based methods, and (4) Hybrid methods. Prevailing literature generally possesses restricted parameters. It furnishes a synopsis regarding techniques for discerning assaults, and only several studies discuss these methods in detail. Most surveys do not fully cover the entire scope of machine learning, deep learning, hybrid, and scenario-based methods, resulting in knowledge gaps in how well they perform. Also, little detailed analysis exists in the areas of addressing current and predicted complications facing phishing attack detection, thus pointing towards a need for additional research in this area.

Cybercriminals were able to successfully scam Facebook and Google out of more than $100 million via an elaborate phishing campaign (Jain and Gupta, 2022) . The attackers fabricated a fake company and employed phishing emails to deceive employees from both tech giants into interacting with them. The U.S. Attorney's Office for the Southern District of New York, this scam tricked employees into performing financial transactions, which ended up costing $100 million between 2013 and 2015. Being multibillion-dollar companies, both firms were victims of this highly successful social engineering attack, highlighting the success of phishing attacks in breaching even highly secure organizations.

(a) In 2016, prosecutors accused Quanta Computer in Taiwan, a partner with Facebook and Google, of creating a fake business unit and a front for crime.
(b) Rimasosk was named the only member of the Board of Directors for this phone company, which was the focal point of fraud activities.
(c) In early 2013, the Rimsausk and their co-prosecutors staged an advanced phishing scheme by developing highly sophisticated fake emails, using the hacked email accounts to manipulate their victims.
(d) The attackers used phishing emails that included fake invoices to initiate contact with Google and Facebook staff, luring them into making spurious payments.
(e) Rimasauskas fabricated agreements, correspondence, and remittance applications. They seemed legitimately endorsed as well as sanctioned via executives also representatives of his fictitious enterprises, thus adding more weight to the scam.
(f) Through his sophisticated scam, by 2015, Rimasauskas had been able to scam Google out of $23 million and Facebook out of $98 million. This case illustrates how email and website-based phishing attacks, which are a specific form of social engineering, can be employed to trick even big businesses out of money.

Data collection procedure for the current Apruzzese et al. (2019) The survey follows the insight that provides intensive information about the phishing attacks. The survey has paid attention to communication channels, target equipment, attack strategy, and counter-types, and 7 communication media used for phishing attacks. The survey has also outlined various target devices, such as individual computers, smart devices, and

various attack methods applied to cellular phones. In addition, phishing techniques are classified into two broad categories: attack launching technology and data collection strategies, appointing cybercriminals to describe various methods. In addition, research involves the insight into the Avaldus Rimasosuscus case, which reflects the harsh negative consequences fishing attacks, especially in social engineering contexts, email, and website-based life conditions showing people. This case stresses that we must comprehend and counter phishing threats since we should have strong cybersecurity. The data compilation procedure integrates details from hypothetical surveys with concrete cybercrime occurrences. The investigation seeks to formulate an exhaustive assessment of phishing methods, resultant effects, and countermeasure effectiveness. The process guarantees exhaustive exploration of phishing attack patterns to understand vulnerabilities better and devise meaningful security measures.

3.7 Data Analysis Techniques

An assortment of methods scrutinized customer support employee data originating from social engineering attacks to obtain statistical evidence concerning results and patterns. The protocols furnished statistical confirmation for outcomes and configurations. Descriptive statistics summarized salient data for attackers by distilling data and yielding prevalence involving attack type, employee role, and targeted information. Using percentages in analysis, we showed what kind of social engineering attacks happened most and what part employees were impacted. Averages gave feet on land as to the norm exhibit being exposed or vulnerable to attackers, and SDs gave us an idea on how these patterns appeared differently among employees.

Statistically speaking this uncovered essential trend including the favorite types of social engineering attacks and common roles of employees targeted. We also did chi-squared tests looking at potential associations between certain categorical variables. For instance, the test would tell if certain attack types were associated with specific roles or the kind of sensitive data targeted and employee department. To look at the data more clearly, some visualization approaches e.g. a bar chart, frequency tables were used. The visuals made it easier for me to see and understand the data trends, which patterns really stood out and stood as proof to effective communication of findings. The comprehensive

statistical analysis provided some of those interesting details about the social engineering threat perimeter that helped understand which soft spots exist with customer support agents and where we might want to invest more in training or protection.

3.7.1 Chi-Square Tests: To analyze associations between:

Chi-Square (χ^2) test of independence was performed to look into the relationships between categorical variables. The test checks independence between occurrence of one categorical variable (employee role) and some other variable (attack type). For instance, the Chi-square was used to investigate if specific employee roles like customer service representatives, technical support staff and billing agents were more frequent targets for phishing, pretexting or baiting socially engineered attack types. By diving into which jobs and roles were getting attacked, the test helped determine if certain roles were more likely as a consequence of their job function. For example, employees in customer service will be the front facing employees and therefore may be more at risk to phishing targeting individual information. Technical support staff might be targeted wit pretexting. The levels of statistical significance of the results whether the odds of an attack type varied by job role so that organizations can tailor security training to their most vulnerable employees

3.7.2 Employee Roles and Likelihood of Being Targeted

This analysis investigates whether social engineering attacks disproportionately target specific employee roles within customer support. The rationale is that certain roles, due to their inherent responsibilities and system access, may present more attractive targets for attackers. For instance, employees handling account administration, billing, or technical support often possess the authorization to modify account settings, process financial transactions, or access sensitive system configurations. This analysis seeks to determine if social engineers strategically target these roles to exploit their access privileges. Understanding such targeting patterns is crucial for developing role-specific security training and access control policies. This analysis investigates whether social engineering attacks disproportionately target specific employee roles within customer support. The rationale is that certain roles, due to their inherent responsibilities and system access, may present more attractive targets for attackers. For instance,

employees handling account administration, billing, or technical support often possess the authorization to modify account settings, process financial transactions, or access sensitive system configurations. This analysis seeks to determine if social engineers strategically target these roles to exploit their access privileges. Understanding such targeting patterns is crucial for developing role-specific security training and access control policies.The Chi-Square test was used to identify if social engineering attacks were disproportionately targeted at certain job positions within the organization. The analysis was done in an effort to determine if attackers targeted employees based on their position and level of access to sensitive data as opposed to using indiscriminate forms of attack. Some positions, like billing agents, account managers, and technical support staff, directly access payment information, customer account information, and authentication credentials and are therefore higher-risk targets. On the other hand, general administrative staff or staff with limited access to core systems may receive fewer attack attempts. By contrasting observed attack observations with what would be observed if attacks were randomly occurring, an assessment as to whether there exists a statistically meaningful correlation between job position and chances of being targeted was ascertained through the Chi-Square test. A strong relationship revealed in the analysis would indicate attackers designate employees according to roles, so organizations must customize security training for high-risk employees. To reduce their increased susceptibility, these people would need more intense training, more stringent access controls, alongside augmented security protocols. In the event that a strong association is not ascertained, this might denote social engineering attacks feature diminished specificity. These assaults impacted personnel across every employment classification without preference. Within such context, fortification is vital. Security policies across an organization are of vital importance., awareness training, coupled with reporting mechanisms. Notwithstanding the test's potential negative indication, the imperative to safeguard private data persists constantly. Active security education, role-specific hazard assessment, and evolving protection strategies stress shielding every worker role. Safeguarding staff roles curtails the frequency of successful social engineering incursions.

3.7.3 Security Measures and Attack Frequency

This section scrutinizes the frequency at which social engineering attacks materialize within implemented security protocols. It assesses if security controls skillfully curtail successful attacks given that they include multi-factor authentication (MFA), educate employees, also report incidents.

This research endeavored to scrutinize how protective procedures influence establishments. It also endeavored to connect these actions with the frequency of social engineering attacks. Particularly, we endeavored to ascertain whether employing multi-factor authentication (MFA), educating personnel, and detailing incidents helped in diminishing these attacks' efficacy and frequency. To assess this correlation, attack rates among groups possessing differing degrees of security enforcement were evaluated using a Chi-Square test. We planned to ascertain whether security protocols along with the rate of attacks possessed some statistically meaningful association. This sought to ascertain whether diverse cybersecurity safeguards adequately deter cyber threats initiated by humans.

If the Chi-Square test resulted in a highly significant outcome, it would be an indication that organizations with effective security controls—like mandated MFA, ongoing security training, and active reporting mechanisms—saw a lower-than-average incidence of attacks. This would identify the protective value of these security controls in preventing unauthorized access attempts, lowering vulnerability to phishing and pretexting, and improving general organizational resistance to social engineering. For example, those organizations that implement MFA as a strict security policy can radically cut credential theft attacks since the attackers would be less likely to breach accounts even when passwords are compromised. Likewise, an organized incident reporting system where employees are prompted to report unusual behavior can catch and nullify penetration efforts before they turn into large-scale security breaches. Alternatively, should the result be a lessened or nonexistent correlation, this may suggest loopholes arose when security policies were implemented as well as indicating that simply embracing security protocols is inadequate: regular enforcement, frequent revision, with continual monitoring are needed so effectiveness may continue.

3.7.4 Chi-Square Test Equation

A statistical technique, the Chi-Square (χ^2) test, ascertains whether there is a meaningful association among two variable sets. It examines whether the observed frequencies in the data differ substantially from the expected frequencies assuming independence. Chi-square test is calculated using the following Eq (1):

$$\chi^2 = \sum \quad \frac{(O-E)^2}{E} \tag{1}$$

where observed frequency and the expected frequency is defined as O and E and the summation across all categories in the contingency table is denoted as Σ.

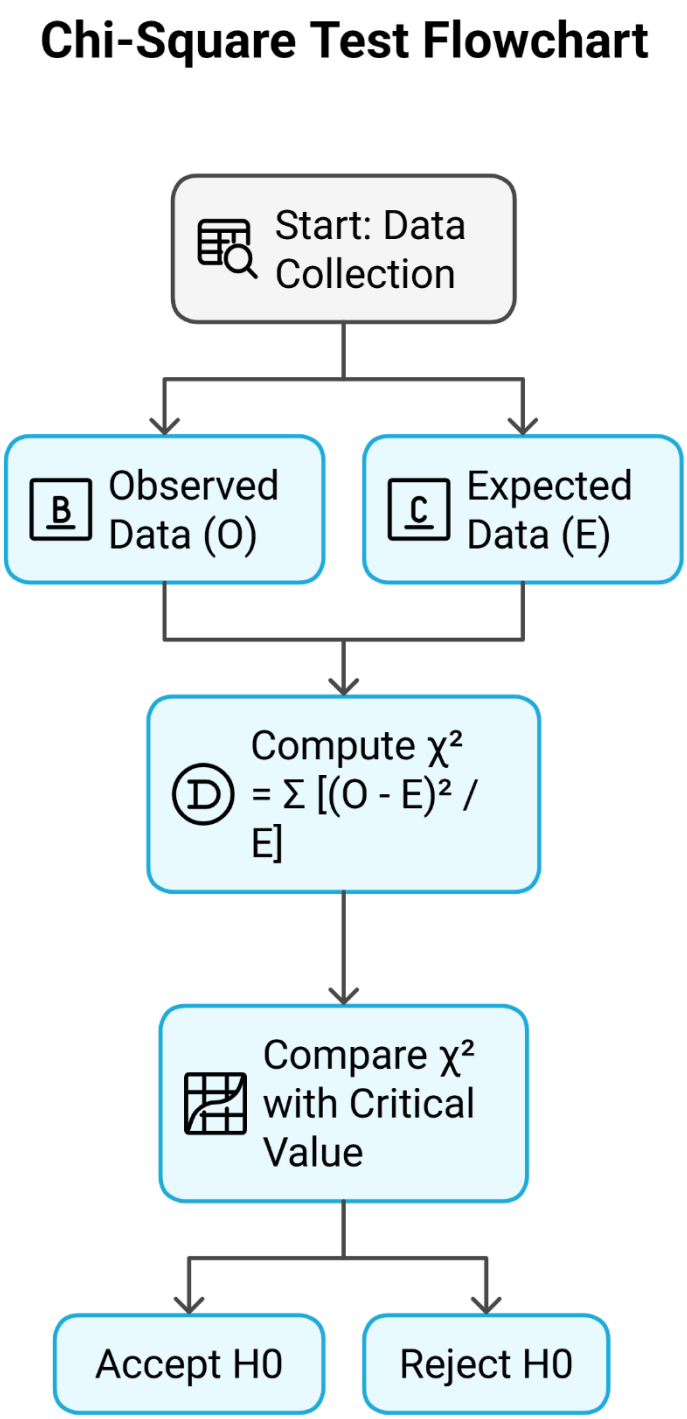

Figure 3. 7: Chi_Sqaure Tesr Flowchart

3.7.5 Step-by-Step Breakdown of the Formula

1. **Observed Frequency (O)**

Empirical values represent tallies documented per classification within a dataset. This is notably accurate within statistical inference, such as Chi-Square testing. They are the concrete instantiation of an incident juxtaposed with probability distributions' hypothetically projected tallies, the anticipated quantities. In the context of the investigation, observed metrics denote how often personnel within diverse positions experienced manipulation exploits. Therefore, ascertaining whether specific positions suffer selective attacker targeting is eased.

For example, in the event the research endeavors to gauge just how social engineering efforts influence technical support, customer services, billing personnel, together with account support employees are affected as well. Workers would undergo an abundance of assaults within each of the observed categories. If 15 incidents were reported by technical support employees, 10 by customer service, and 5 by billing staff, these would be the observed values for the analysis. Scientists contrast these metrics with the predicted quantities to ascertain something. They may ascertain whether employee roles bear a substantial statistical correlation to the likelihood of being victimized.

Values observed are very important in recognizing patterns and trends of cybersecurity attacks. When specific job roles repeatedly exhibit higher attack rates, it would denote that employees possessing greater access to sensitive customer information are explicitly targeted by the attackers. Social engineering incursions happen without distinction when attacks get apparently apportioned among differing occupations. Through these counts captured in records, organizations can sharpen their cybersecurity policies by targeting role-based security training, access control measures, and improving incident response to counter future attacks efficiently.

2. **Expected Frequency (E)**

- We compute the anticipated frequency. We posit **no relationship** subsists amid the two variables. This can be calculated using the following Eq(2):

$$E = \frac{(Row\ Total \times Column\ Total)}{Grand\ Total} \quad (2)$$

- This ensures that the distribution is based purely on proportions rather than any real relationship.

In our analysis, anticipated frequencies aid examination of whether employee roles affect the incidence of social engineering attacks. Attacks, for instance, if distributed haphazardly by fortune, each employee position would correlate to a forecasted quantity of attack episodes. This value represents a portion of the complete data set. If observed data substantially varies from the expected values, it indicates that particular employee roles are disproportionately targeted by attackers. This statistical method aids in determining if cybercriminals target specific job positions, including technical support, account help, or billing personnel, because they may procure private intelligence. If the Chi-Square test is statistically significant, then attackers do not target employees indiscriminately, but rather strategically target particular job titles. This observation is vital to formulate particular security stipulations such as firmer access control protocols, strengthened oversight for perilous duties, and role-reliant cybersecurity instruction. Nevertheless, should people not interface effectively, this implies perpetrators conduct social manipulation indiscriminately, thus validating the necessity of rendering entire organizations security mindful rather than confining this to particular positions exclusively. This inquiry uses anticipated frequencies, and it furnishes substantiated data. This data pertains to the hazards that social engineering introduces. Subsequently, organizations may embrace powerful, fact-based security protocols against cyber threats.

3.8 Summary

This research framework presents an organized method to evaluate the consequence and frequency of social engineering exploits upon mobile service vendors' client assistance personnel. Associations among attack categories, specified positions, and protective actions are evaluated through illustrative charts and chi-squared analyses; the research uses questionnaire-derived information gathering and focuses on diverse worker functions. The analysis is focused upon how exactly we discern the pattern for general attack, how we assess the vulnerability of specific employee roles, as well as how we determine whether the existing security protocol is indeed effective. The investigation explores the correlation between security protocols and incidence of

assaults. Practical perceptions seek to augment organizational protection consequently. For an effective diminishment of social engineering threats, this will aid mobile service providers in improving employee training, strengthening safety policies, and developing stronger event reaction mechanisms.

Chapter 4

Result and Discussion

4.1 Overview

This chapter furnishes an exhaustive dissection of data procured from respondents employed in diverse customer support roles among mobile service providers. This analysis endeavors chiefly to spotlight key trends and perceptions concerning social engineering offensives, the kinds of data routinely assailed, staff members most vulnerable to these offensives, and how competently these entities execute protective protocols. Regarding lucid comprehension about social engineering hazards and breadth within the mobile service milieu, descriptive and inferential statistical techniques enable the analysis. This chapter scrutinizes the demographic distribution of survey participants along with their particular functions for customer assistance. Subsequently, it scrutinizes the frequency together with the category of social engineering. Assailants frequently endeavor to procure data. They pursue specific consumer particulars, account identifications, monetary intelligence, and additional confidential facts. Grasping the degree of exposure is vital to this aspect and a range of data connected with the chief aims of social engineering crimes.

Furthermore, the chapter ascertains if social engineering attacks have an elevated likelihood to target specific job roles within customer aid, for example technical support, account assistance, dealing with complaints, as well as management. They acquire it through lower statistical tests like the Chi-Square tests to determine how employee job correlates to the likelihood of being targeted, and to desire to accomplish the kind of information attackers. The chapter additionally explores whether the frequency of social engineering exploits correlates with implementing organizational safety protocols and incident reporting initiatives. This provides perception into the effectiveness of those regulations. The assessment additionally scrutinizes institutional security protocols in conjunction with how competently occurrence notification diminishes confidence trick assaults. This assessment determines whether people embrace stringent security protocols. Additionally, personnel chronicle questionable conduct to substantially lessen the incidence of successful social engineering offensives. The investigative team

unearthed perceptive intelligence. People may execute proactive safeguards, strengthening institutional security from incursions.

Furthermore, conclusions emphasized the necessity of specific staff training and sensitization programs focused on minimizing social engineering threats. The research places emphasis on the organizational culture in facilitating an environment that encourages safety awareness through cautious and active employees protecting personal customer data. It also accentuates that organizations should strengthen internal controls, should revise the safety protocol routinely, and should diminish the consequences from social engineering threats so they might foster a climate of event reporting and transparency. The chapter scrutinizes data systematically and exhaustively. This analysis furnishes practical perceptions that can enable mobile service providers to fortify their defense measures against social engineering attacks. Statistical experiment outcomes, notably regarding autonomy, present factual confirmation concerning the nexus between penetration testing, staff directories, classifications of pinpointed intelligence, and social engineering intrusion frequency. This chapter uncovers important discoveries while also gauging strong security substantially coupled with intervening tactically for safeguarding the organization against susceptibility to social engineering attacks.

4.2 Descriptive Analysis

Descriptive analysis stresses data more throughout social engineering incursions, their customer support job designations, and common inclinations stressing information from participants. The objective of this section is to stress the frequency distribution of the meaningful variable as well as scrutinize the general trends that emerged from the data. Elucidating examination endeavors to show the central perception into the characteristic of intended data via social manipulation aggressors. It mirrors the degree of exposure regarding distinct customer support positions at mobile service provider organizations.

The below Table 4.1 shows the frequency distribution of the information sought by the respondents as mentioned:

Table 4. 1: Frequency Distribution of Targeted Information

Targeted Information	Frequency (n)	Percentage (%)
Personal details (Name, Address, Contact number, etc.)	21	35.0%
Account details (Login credentials, Billing info, etc.)	6	10.0%
Financial details (Bank account, Credit card details, etc.)	1	1.7%
Confidential customer information	11	18.3%
Other account-related information	21	35.0%
Total	60	100.0%

Table 4.1 Frequency distribution of information targeted showed that attackers direct the majority of social engineering attacks toward obtaining individual customer information representing 35% of total responses. This classification includes sensitive data incorporating name, address, contact number, identity number, as well as account-related data. Typically, assailants will manipulate specific minutiae toward evil operations. These pursuits include identity pilfering, procurement of accounts, or monetary deceit. This is a big concern for mobile service providers because customers share their private information with these organizations. The study also demonstrated that the account information was the second most hit category at 10% of the responses. These include login credentials, billing data, and account management details, which, when exploited by attackers, can use them to obtain access to accounts, swap service plans, or perform illegitimate transactions. Furthermore, financial data including bank account numbers, credit card information, or payment history, was targeted in 1.7% of the reports, also this targeting reflects the express attempt to perpetrate financial fraud.

Distribution of Employee Roles in Customer Support

The study captured data originating from employees because they were participating in diverse roles such as technical aid, account assistance, billing service, customer service, along with management. Observed frequency distribution signaled the greatest respondent percentage existed within technical aid roles. They comprised 18.3% of those surveyed. These employees mainly handle technical issues related to service outages, network configuration, hardware problems, and technical troubleshooting. Intruders frequently find that technical support personnel represent a worthwhile objective regarding internal frameworks since they possess avenues into the core infrastructure as well as specialized architecture.

The second-highest portion of employees, 15%, were engaged in account assistance, including customer accounts, billing enquiries, and planning changes. In this role, employees are often targeted to obtain billing and account management information, allowing the attackers to manipulate account settings or execute fraud transactions. Customer service employees are responsible for 13.3% of the respondents, also they chiefly tackle customer questions, solve complaints, as well as furnish information regarding service. Since these client interactions render them exceedingly susceptible against social engineering, attackers impersonate clients to glean private data. Illustrative assessment considerably ascertained the allocation of employee functions inside the Customer Assistance Department. It also pinpointed whether social engineering exploits made each particular position more susceptible. The following Table 4.2 presents the distribution of employee roles in customer aid:

Table 4. 2: Frequency Distribution of Employee Roles in Customer Support

Employee Role	Frequency (n)	Percentage (%)
Technical Support	11	18.3%
Account Assistance	9	15.0%
Customer Service	8	13.3%
Handling Complaints	10	16.7%

Billing Service	6	10.0%
Data Handling Issues	2	3.3%
Plan Change and Upgrade	1	1.7%
Management	1	1.7%
Network Coverage Service	1	1.7%
Personal Details Handling	2	3.3%
Escalate Complex Issues	1	1.7%
Total	60	100.0%

Table 4.2 shows the distribution of the roles of employees in customer support, displaying the ratio of employees to different job roles within the company. The statistics indicate that someone allocated the 60 employees among different job areas of customer support, also this offers information regarding the workforce structure, furthermore, someone concentrates on duties. The allotment of duties constitutes a priority too. Technical Support constitutes the paramount proportional depiction within the enumerated occupations at 18.3%. This calculation represents 11 staff members within the entire staff. This suggests maximum attention towards technical problem-solving, including troubleshooting, equipment setup, and connectivity assistance. Complaint Handling comes second, representing 16.7% (10 staff), reflecting the company's priority on complaint resolution and the escalation of unsolved grievances. Customer Service and Account Assistance positions constitute 15.0% (9 employees) and 13.3% (8 employees), respectively, indicating their key role in attending to customer accounts, billing inquiries, and overall inquiries.

Other job titles, including Billing Service (10.0%), include customer payment processing and billing issue resolution, while Data Handling Issues (3.3%) are dedicated to protecting and handling customer information. Specialized jobs like Plan Change and Upgrade, Management, Network Coverage Service, Personal Details Handling, and Escalating Complex Issues each have between 1.7% and 3.3% of the job market. These jobs, although in less proportion, are highly essential for particular activities like altering customer plans, maintaining service quality, and dealing with customer sensitive information. The frequency distribution indicates the majority of the employees to be

carrying out core customer care activities, with technical assistance, complaint handling, and account aid being the predominant jobs. Specialized jobs point toward an organized scheme of tending to differing customer demands. Realization of this distribution assists in workload distribution analysis, high-risk areas detection for cybersecurity threats, and the formulation of specialized training programs to improve service efficiency and security awareness.

Relationship Between Employee Role and Targeted Information

Descriptive analysis further revealed that while the attackers often targeted personal information, they did not ban their attention on a specific employee role. This shows that attackers deploy social engineering strategies in various customer aid roles without preference. However, employees in account assistance, billing service, and technical support roles reported a high frequency of social engineering efforts. This further indicates that the employees with access to sensitive customer information are naturally at high risk. In addition, handling complaints and resolving technical issues emerged as an important vulnerability area, where attackers copy customers or employees to extract confidential data. For instance, assailants can pose as real customers requesting password resets, billing modifications, or service upgrades to get unauthorized access to customer accounts.

4.3 Hypothesis Testing

This section presents the results from the hypothesis test undertaken to pinpoint vital associations between security processes impacting together with diminishing employee roles, targeted information, also social engineering attacks. The study's objectives informed tests of three meaningful hypotheses. The Chi-Square Test is the foremost inferential statistical technique that was used. The analysis intends to scrutinize the arrangement's efficacy concerning safety, a target's vulnerability, together with the attack's intensity.

The Chi-Square Test represents a statistical assessment. Investigators use it so they can ascertain the vital association between both collections of variables. This research employed the test:

Employee role and type of social engineering attack

This was carried out to determine whether different job roles have different types of social engineering attacks linked to them. Employees in different roles may face some forms of threats depending on the type of job they do along with their level of access to sensitive information. Technical support employees remain susceptible to phishing emails resembling IT support queries. Deceptive invoices might victimize personnel handling payments. Organizations scrutinize the statistical relevance of those associations. Subsequently, they are able to ascertain elevated-risk employee cohorts and furnish commensurate security instruction.

Employee role and likelihood of being targeted

This study was intended to determine if some job titles are more prone to cyberattacks. Social engineers typically target employees with access to useful information, thus making some job titles more exposed to attack. For example, account support staff dealing with customer information might be targeted more than complaint handling staff dealing with broad customer queries. Role-specific security awareness programs are essential when the Chi-Square Test reveals a substantial correlation, which indicates that attackers selectively target employees based on their positions.

Presence of security procedures and frequency of social engineering attempts

The research also gauged if someone mandates security protocols like two-factor authentication (2FA) when seeking to reduce the frequency of social engineering exploits, alongside access oversight and staff instruction. The Chi-Square Test assessed attack rates among organizations or departments. Several were missing strict security protocols, yet others possessed them. Should it prove statistically important, an association would denote organizations enforcing security protocols effectively experience a reduced incidence of social engineering incursions, thereby substantiating that cybersecurity policies must curtail attacks.

Per p-mam, testing findings were considerably illuminated at 0.05. The p-value denotes statistical importance between the variables when it is below 0.05. The variables then exhibit a statistically meaningful correlation. A substantive correlation is absent if the P-

value exceeds 0.05. The subsequent segment explores the findings. The hypothesis test is expounded upon in that section.

4.3.1 Explanation of Variables in Conceptual Framework

Independent variables coupled with dependent variables comprise a pair of variable classifications regarding the current study's conceptual framework. The aims of the study established these variables. Statistical experiments, particularly the Chi-Square assessment, scrutinized those connections. A variable is meaningful toward comprehending aspects affecting safety measure influence when diminishing social engineering intrusions, pinpointed data, and reducing attacks. The following Figure 4.1 refers to the conceptual structure:

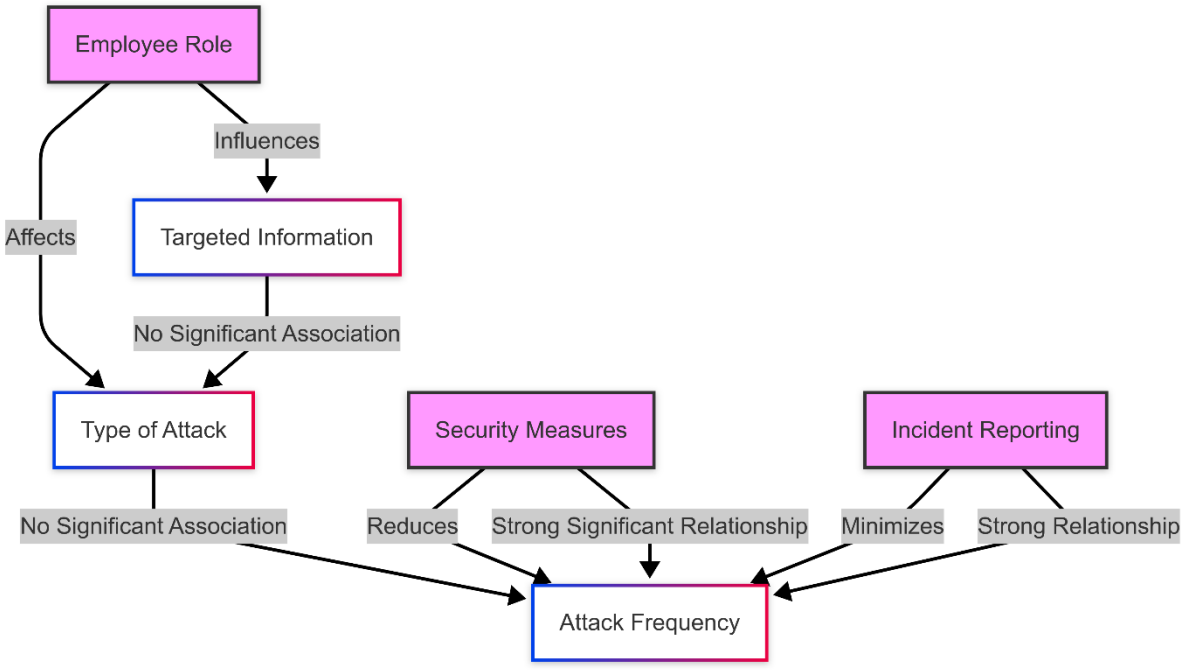

Figure 4. 1: Conceptual Framework

The figure 4.1 constitutes a depiction of just how disparate organizational variables can interact, along with how they impact the prevalence of social engineering attacks at mobile service providers. The figure is mainly contingent upon attack frequency augmenting or diminishing via the contribution of employee roles, information targeted, attack type, security protocols, and reporting of incidents. Initially within the depiction, Employee Role importantly contributes to defining the characteristic of designated information. The positions workers hold within an organization impacting their data

access can subsequently render them vulnerable to social engineering ploys. Nonetheless, Employee Role does not strongly correlate. Type of Attack does not powerfully associate either, which signifies that employee role does not determine explicitly the type of attack though it does target the information. The diagram depicts Employee Role is not in direct correlation with Type of Attack. This implies that social engineering offenses may materialize diversely. The employee's position has no bearing upon the forms assaults assume. This suggests that social engineering assaults may exhibit diverse forms regardless of the employee's function.

The types of attacks (e.g., phishing, vishing, or pretexting) are not strongly associated with the employee role or the targeted information, despite the fact that the Targeted Information (e.g., customer information, financial data, etc.) is affected by the employee role. This suggests that attackers may employ any attack technique, regardless of the employee's role.

Going forward, the diagram indicates there are 2 key organizational variables directly influencing Attack Frequency: Security Measures and Incident Reporting. Security Measures, encompassing technical controls, data encryption, access controls, and staff training, exhibit a significant positive relationship in lowering attack frequency. That is, having effective security measures in place throughout the organization strongly reduces the likelihood of successful social engineering attacks. Contrarily, Incident Reporting is crucial in reducing attack frequency. Reporting suspicious activity, phishing, or abnormal behavior by employees fosters a good relationship with attack frequency reduction. This illustrates that the more employees actively report possible threats, the lower the attack frequency. In the end, the diagram highlights that Employee Role indirectly affects Attack Frequency via Targeted Information and Security Measures. Type of Attack is not strongly associated with Employee Role or Attack Frequency. The two major factors that significantly minimize the attack frequency are good security measures and incident reporting. In that these dual elements are integrated, a strong protective measure versus social engineering incursions is rendered, with its ultimate effect being to secure the establishment's confidential data. In the subsequent section, there is an explanation of independent as well as dependent variables in greater detail. Grasping their importance is important to this analysis.

4.3.2 Independent Variables

Independent variables are variables in dependent variables that instigate, propel, or influence fluctuations. Autonomous factors either augment or diminish social engineering assaults. As per this investigation, these determinants transpire inside the cellular communication supplier milieu. This study includes three major independent variables as follows:

a) **Employee Role**

The function of the employee refers to the job status or responsibility organised by the defendant within the mobile service provider organization. Since diverse duties exist, customer information, technical aid, with interior system infrastructure access are distinct for the employees, so particular roles become more vulnerable to social engineering attacks than others. Within social engineering incursions, clients, utility personnel, or IT support staff are frequently misrepresented. Due to this, perpetrators procure private client specifics. This replication eases that removal. The study's intention consequently verifies the staff (such as technical support, account assistance, dealing with complaints, etc.) were targeted more often than others.

Roles Considered:

The study covers several significant job positions that are vital in customer support provision and smooth functioning in a service provider. They are important components in fulfilling customers' needs, problem-solving, and service provision. The following is a thorough description of the jobs covered under the study:

- Technical Assistance: Staff working under this position focus on solving and fixing technical problems faced by the customers. Their responsibilities can range from setting up equipment, troubleshooting connectivity issues, remote support, and making sure customers have a smooth experience with the products and services of the company. The workers usually handle network-related issues, device failures, and software or hardware-related questions. Their skills are essential in keeping customers satisfied, since customers engage support most often on account of technological quandaries.

- Account Support: This position is dedicated to handling customer accounts and responding to different account-related questions. Staff in this category support customers with billing information, subscription plans, payment changes, account verification, and updates to personal data. They ascertain that customers gain access to their services without any interruption also helping them to upgrade, downgrade, or terminate their plans. Since stewardship of accounts is delicate and monetary exchanges materialize, staff in this role must be careful and safeguard client details via adherence to protective protocols.
- Customer Service: Customer service staff members represent the foremost conduit of interaction toward patrons when they solicit standard assistance. They have the responsibility to furnish answers to queries, they aid customers to traverse diverse procedures, and they support those customers with prompt utility. Customer support representatives can be integrated within other functions such as account assistance and complaint resolution. That circumstance arises because these delegates must possess comprehension regarding each aspect of the company's operations. Their duty mainly entails satisfaction enhancement for customers via efficiently solving concerns as well as forwarding customers if required.
- Billing Service: The staff performing the billing service role is responsible for customer payments, transaction handling, and problem-solving related to billing. They assist customers in navigating their bills, explain charges, rectify mistakes, and settle payment conflicts. They ensure billing processes remain seamless and error-free for customers' consumed services. Since billing errors may lead to dissatisfaction and increase conflicts, workers occupying this role should be detail-oriented and able to answer financial questions correctly.
- Complaint Handling: The job requires dealing with customer complaints and addressing intricate problems, which might involve escalation. Workers serving in complaint handling engage directly with consumers who have issues with services, billing issues, technical issues, or other issues. They aim to offer solutions, deliver customer satisfaction, and avoid repeat issues. Complaint handling is key to good company reputation and customer loyalty. Personnel that

operate within this capacity may need to communicate excellently also solve problems for addressing customers' issues efficiently.

These roles all factor within a service provider. These roles are critical to the entirety of customer support's function. Through efficient handling of technical problems, account inquiries, customer contacts, billing issues, and complaints, employees ensure high standards of service, enhance customer satisfaction, and improve business operations.

Relationship to Dependent Variables:

The research had previously assumed that some employee positions—e.g., technical support, account support, or billing service—would be more likely targeted by social engineering attacks because of their direct handling of sensitive customer data. Yet the results from the Chi-Square Test, which had a p-value of 0.993, neglected to exhibit any statistically important association. This existed among employee position coupled with the type of social engineering attack experienced. Hence, assailants do not single out some specific employment positions but rather employ random attack methods throughout the company.

One plausible rationale for this finding is that human psychology manipulation predominates over social engineering more than role-specific access to information. The attackers use phishing emails, vishing calls, together with pretexting methods since such methods can dupe employees within any position, not simply those possessing access to sensitive customer data. Cybercriminals employ ubiquitous, adaptable techniques instead of designating their intrusions according to a precise vocational role. They strive to manipulate every susceptible employee within the company, implying such conduct. Cybersecurity awareness education is used pervasively. This could be the reason attack rates failed to fluctuate among roles. Their susceptibility toward social engineering attacks might become uniform. This may transpire should each person within the firm undertake identical education and possess equivalent standard security protocols. This inference elucidates how protective protocols advantage the entire institution instead of solely shielding critical positions. Organizations should prioritize ongoing training of employees, strong access controls, and active incident reporting to reduce the risks of indiscriminate social engineering attacks.

b) Security Measures

Security controls are the organizational policies, technical controls, and preventive measures adopted to protect customer data from unauthorised access, data loss, and social engineering attacks. Security controls can comprise two-factor authentication, tight access controls, security training initiatives, and regular audits. The research aims to assess whether having strong safety controls has a significant impact on reducing the number of social engineering attacks. It was assumed that organizations implementing strict security policies would witness less social engineering attempts compared to individuals with the least security controls.

Security Measures Considered:

To strengthen cybersecurity and safeguard sensitive customer information, this study has contemplated many security controls. These safeguards are created to curtail the menace that forbidden agents gain access to, violate, and assail data inside the corporation. The following are the most critical security controls considered in the study, along with their significance and impact on organizational security:

i. Two-Factor Authentication (2FA):

Two-factor authentication (2FA) is a key security process that has the goal to give an additional security level at the time that employees log on to confidential systems or customers' data. Not just a password, but an additional authenticatable mechanism is needed via 2FA prior to user fulfillment like a temporary PIN within the mobile phone, biometric sign-on (fingerprint, face), or security questions. Confidential information is accessible to authenticated personnel exclusively, even when login information has been jeopardized. 2FA substantially reduces the hazard from forbidden access. It also protects against cyber-attacks such as brute-force attacks, along with credential theft.

ii. Data Privacy Training:

One way to effectively cease cyber attacks involves educating as well as alerting employees. Data privacy training is teaching employees how to handle sensitive customer data using best practices, recognizing potential risks (phishing and social

engineering attacks), and following company policies in safeguarding information. Training can cover issues such as password management, how to recognize a suspicious email, secure storage of data, and data protection law compliance. By equipping employees with the necessary knowledge and competencies, organizations are able to minimize the possibility of human mistake leading to security violations.

iii. Access Control:

Access control policies enact constraints restricting staff access to confidential customer information so only permitted staff access or alter private information. This safeguard defends private intelligence. Forbidden internal personnel cannot gain entry to it, also external entities cannot malevolently assail it. Access protocols can feature role-oriented access regulation, or RBAC, in which authorization depends on activities necessary for doing the task, alongside constrained rights guidelines in which admittance is solely as wide-ranging as the worker requires for undertaking labor. Strict access policies implemented reduce the likelihood of data leakage, insider attacks, and accidental disclosure of confidential information.

iv. Event Reporting

Making employees report suspicious behavior or out-of-the-ordinary conversations is an in-time security measure that helps identify potential threats early. Event reporting involves instituting a system whereby workers can report security breaches, phishing attempts, or suspect activities without facing retaliation. organizations can establish anonymous reporting mechanisms and clearly communicate what defines a security threat. By such a culture of security responsibility and awareness, the companies are able to nip risks in the bud before such risks had mushroomed into major security breaches.

Relationship to Dependent Variables:

The consequences of the Chi-Square Testing showed a strong significant relationship between the presence of safety measures and the frequency of social engineering attacks (p-value = 0.001). This confirmed that organizations with strong security measures experienced fewer social engineering efforts.

a) Incident Reporting

Incident reporting refers to any suspicious activities, phishing efforts, social engineering attacks, or the practice of employees reporting data violations to their management or security team. The purpose of the incident reporting is to prevent further damage, have high officials increase the issue, and diminish social engineering attacks' success rate. The study envisaged that increasing incidence reporting within the organization could significantly reduce the frequency of attacks. When employees immediately report suspicious emails, phone calls, or customer-copying efforts, it enables the organization to take preventive measures and protect customer data.

Relationship to Dependent Variables:

The association between social engineering attacks frequency and incident reporting was examined using the Chi-Square Test, which identified a significant relationship with a p-value of 0.003. Diminished successful social engineering incursions often transpire within enterprises where personnel communicate security breaches. Effective incident reporting is crucial in the discovery, containment, and prevention of cyber attacks before they become full-blown breaches. When employees actively report phishing emails, calls, or attempts at unauthorized access, security teams can rapidly react, investigate threats, and implement necessary countermeasures. One of the reasons for this connection is that an open security awareness and reporting culture discourages attackers from repeatedly targeting the same organization. When there are regular reports of security incidents and documentation, the attackers may be less likely to exploit vulnerabilities as organizations become more prudent in their defence systems. Security teams gain assistance via routine reporting for purposes of tracking attack patterns so as to recognize vulnerabilities and improve security policies with the goal of reducing attack likelihood. Besides, the strong correlation between decreased attack frequency and reporting of incidents proves the worth of employee engagement in cybersecurity. Businesses that foster an environment in which reporting is not punishable and that train employees on guidelines for detecting and reporting threats will be more successful in having stronger defenses against social engineering tactics. Through the integration of incident reporting systems, live threat analysis, and security

awareness programs, organizations can implement a strong security framework that effectively combats cyber threats and degrades the social engineering attacks' effects.

4.3.3 Dependent Variables

Outcomes swayed by worker roles, security protocols as well as incident report procedures represent the dependent variables inside this study. The subordinate variables are contemplated. They include the frequency of social engineering attacks, attack success rate, and types of information attacked by the intruder. These variables help quantify the extent of social engineering threats within the company and how different components sum up or mitigate these threats.

One of the key dependent variables is the incidence of social engineering attacks, showing how regularly employees are targeted via phishing emails, vishing phone calls, or other deceptive techniques. This variable explains whether particular employee roles or organizations with some security controls are more or less susceptible to constant attacks. Increased frequency might reflect laxities in the incident reporting culture, security policies, or employee awareness of an organization, while lower frequency may suggest more preventive mechanisms and security awareness initiatives.

The second significant dependent variable is the success rate of social engineering attacks, which reflects how often attackers are able to gain access to sensitive information or manipulate employees into performing unauthorized tasks. The metric assesses incident response procedures, access controls, alongside security training effectiveness. Entities possessing strong protective protocols along with recurrent staff instruction shall exhibit a diminished incidence of malicious intrusion. Elevated violations, nonetheless, can occur for establishments that possess deficient security doctrines.

Lastly, the types of information that attackers target fundamentally hinge. Cybercriminals might target personal customer data, financial data, account data, or billing data because that hinges on their objectives. Considering that organizations comprehend which data are most frequently targeted, they can institute more efficient security protocols, curtail access to private data as well as enlighten employees on how to protect valuable information. The study furnishes important details concerning the

propensities for social engineering assaults. Via analysis regarding these variables, existing security controls' efficacy was determined:

a) **Type of Attack**

The attack type indicates the particular kind of social engineering tactics employed by the attackers to deceive employees and extract sensitive data from mobile service providers. These attacks are aimed at exploiting human weakness and accessing confidential information. The most frequent type is a phishing email, whereby the attackers had issued a bogus email to receive account details, personal information, or financial data of genuine institutions to defraud employees. Voice phishing, in which attackers undertake simulated telephone calls for customers, technical support representatives, or authorized staff to dupe employees into sharing the account information, password, or billing information, is another widespread practice. Furthermore, pretexting represents another common technique as well as, through it, perpetrators fabricate spurious narratives or feign authorization to obtain private details, login identifications, or confidential firm records. These social engineering attacks are artfully designed for exploiting the trust and human error factor. Because of this, data infringements or fraudulent actions ultimately materialize.

Influence by Independent Variables:

The study aims to ascertain if a specific class of social engineering intrusion rendered certain employment positions more susceptible. Nonetheless, the Chi-Square Test (p-value = 0.993) evinced that employee roles and types of attacks possessed no important association. This suggests the attackers use disparate methodologies coupled with an absence of targeting of particular positions.

b) **Targeted Information**

The targeted information refers to sensitive data that the objective of social engineering attackers is to get from employees working in mobile service provider organizations. This information typically includes personal data such as full name, address, phone number, together with identity information, which could be used for account acquisition or identity theft. Another vital classification of accounts constitutes credentials, and

credentials include usernames, passwords, also account particulars that may be employed for achievement of unsanctioned ingress into attacker customer accounts or toward perpetration of deceitful dealings. Furthermore, assailants commonly aim toward monetary data like bank account figures, credit card specifics, plus payment histories. They do this for thievery and perpetration of financial fraud, illicit transactions, or identity theft. Getting access to this sensitive information enables the attackers to manipulate customer accounts, change service plans, or misuse financial resources, which pose a significant security threat to both the organization and itsfrequency customers.

Influence by Independent Variables:

The study assessed the consequence of differing employee positions. The consequence rested upon the nature of specified detail. However, the Chi-Square Test (p-value = 0.801) showed no important association, showing that the attackers target any available information regardless of the employee role.

c) **Attack Frequency**

The frequency attack refers to the rate at which employees face social engineering efforts within mobile service provider organizations. It measures variable measures of how often the employees face pretexting efforts to obtain phishing emails, wish calls, or sensitive customer information. The volume of such attacks was assessed on a scale, including daily, weekly, monthly, etc., to determine the level of exposure the employees face. The of the attack is greatly affected by two major factors: the presence of safety measures and the reporting of the event by the employees. organizations with strong safety measures, such as two-factor authentication, employee training, and data access control, usually experience a low frequency of social engineering attacks. Similarly, when employees are encouraged to report suspicious activities or potential security violations, it leads to a decrease in successful social engineering efforts. Therefore, reducing the frequency of the attack is directly associated with the organization's active security infrastructure and event reporting culture, which ensures better safety of sensitive customer information.

Objective 1: Identifying Common Social Engineering Attacks

The first hypothesis required an examination to probe for a prominent association within an employee's role and a social engineering attack's type. This hypothesis intends to ascertain if personnel occupying particular positions, including tech support, account assistance, or client relations, were more susceptible to focused offensives like pretexting, wishing calls, prescriptions, or fishing email. The hypothesis was created with a zero hypothesis (H_0) that articulated there is no meaningful correlation between the role of an employee as well as the type of social engineering attack; the alternative hypothesis (H) posited that an important correlation does exist, implying that certain roles may be more susceptible to particular attack types. A p-value equaling 0.993 greatly exceeds the importance threshold of 0.05, so this outcome implies something. Precisely, the outcome evinces that there is no significant correlation between the office of a worker and the form of social manipulation offense. This outcome implies that social engineering perpetrators do not always single out a definite position inside the organization, but commonly accost and single out any worker possessing access to sensitive information. The **Chi-Square test** produced the following result:

Table 4. 3: Chi-Square Test Results for Employee Role and Encountered Attack Type

Test Statistics	**Value**	**Degrees of Freedom (df)**	**p-value**
Pearson Chi-Square	257.214	315	0.993
Likelihood Ratio	144.755	-	-
Linear-by-Linear Association	14.147	-	0.000
Minimum Expected Count	0.02	-	-

The table 4.3 presents the outcome of a Chi-Square assessment designed to investigate the association between the kinds of social engineering attacks employees encounter

and their position. The test statistics shown include the Pearson Chi-Square, the Likelihood Ratio, the Linear-by-Linear Association, and the Minimum Expected Count, along with their corresponding values, degrees of freedom (df), and p-values where relevant. The Pearson Chi-Square statistic that evaluates if categorical variables exhibit independence, has a value of 257.214 with 315 degrees of freedom. TAt 0.993, the corresponding p-value exceeds the standard importance threshold of 0.05 substantially. This indicates a statistically important correlation fails to materialize amid a worker's position and the mode of assault suffered. The apportionment of attack categories does not considerably diverge for the reason that the employee's function does not make it deviate. Social engineering attacks, to put it concisely, seem to affect workers at an equal rate throughout diverse positions instead of focusing on one particular role. The Likelihood Ratio test serves as another method to assess the relationship between categorical variables though this table does not indicate the degrees of freedom nor does it include the p-value. This implies the likelihood ratio may not have been fully calculated or was considered unnecessary for interpretation in this instance. Generally, this test would complement the Pearson Chi-Square by assessing how likely the observed data would occur under different models, but without further details, its contribution to the overall analysis remains ambiguous. The Linear-by-Linear Association test, which investigates whether there is a trend or directional correlation of the variables, has a value of 14.147 and a p-value of 0.000. This points to a statistically significant linear relationship between employee roles and the probability of confronting specific types of attacks. Unlike the Pearson Chi-Square test, which looks at overall independence, this result indicates a more nuanced relationship.

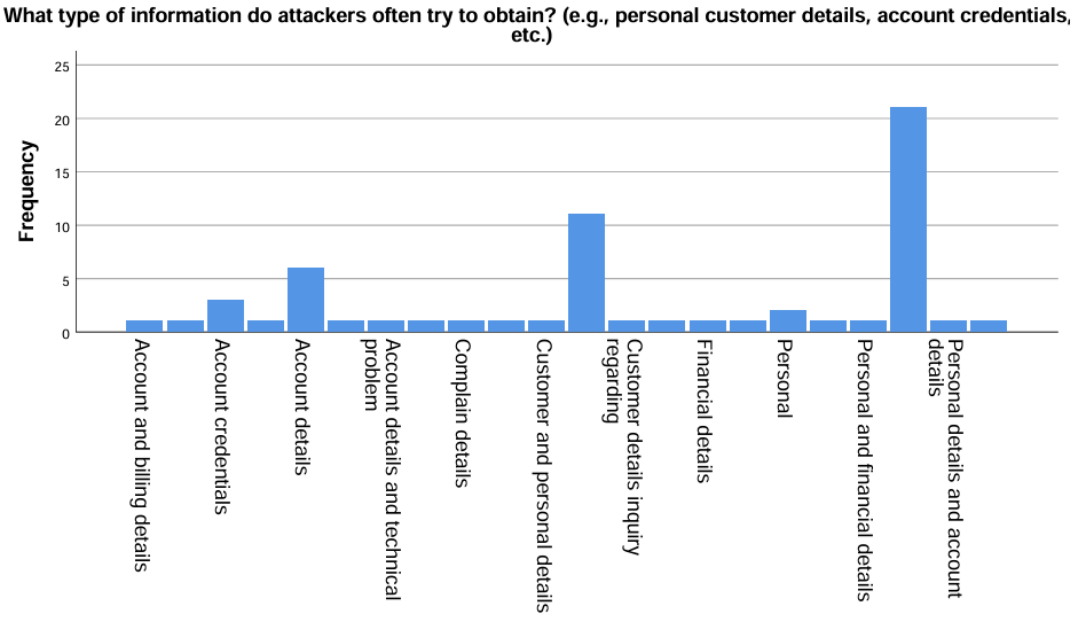

Figure 4.2: Type of Information do attackers often try to obtain

Figure 4.2 depicts the forms of data that perpetrators commonly pursue via diverse social engineering schemes, such as phishing, vishing, or pretexting. The x-axis delineates disparate classes of information that are frequently targeted. The list includes account along with billing details, account credentials, account specifics, technical issues germane to accounts, complaint information, customer plus personal details, inquiries concerning customer details, financial information, personal information, personal and financial details together, also personal details and account specifics. The y-axis represents the frequency of these attempts, showing how often attackers try to obtain each type of information. The highest frequency is noted for personal details and account specifics, surpassing 20 occurrences, indicating that attackers particularly focus on a mix of personal identity and account information, as it grants extensive access to victims' financial, personal, and service-related assets.

The second most frequently targeted category is customer and personal information, since around 13 occurrences reveal perpetrators commonly seek fundamental details like name, phone number, and address. Subsequently, perpetrators could exploit that material in identity theft scenarios or during supplementary social engineering schemes. Account information by itself has a moderate frequency of about 7 instances, indicating

the significance of basic account information for unauthorized access. Account credentials like login names and passwords, and financial information seem to have less frequency of approximately 3 to 5 instances, indicating that the attackers prefer to get a mix of personal and account information rather than isolated credentials. Personal information and financial information have a frequency of approximately 6, indicating that the attackers also derive substantial value from financial information when mixed with personal information. Information regarding grievances, technical impediments, or common patron queries has limited incidence. Clearly, assailants do not perceive great benefit from such data, contrary to private or financial details. The chart evinces that organizations acutely require heightening their security protocols, including authentication via multiple factors, encryption of sensitive information, also instruction for employees regarding recognizing social engineering attacks. Additionally, establishments must ensure clientele understand they must protect private and financial information so they can avert potential privacy violations. This observation also highlights the significance of having a strong incident response mechanism in place to rapidly contain the effect of any possible information breach to ensure customer data security and limit financial losses.

Objective 2: Identifying Most Targeted Employee Roles and Information Sought

The second objective is to discern whether social engineering attacks tend to target particular employee roles throughout mobile service providers and determine if the attack type and target information share a prominent connection. We conceived this aim upon a null hypothesis (H_0). It conveyed that there is no substantive connection between an employee's function and the probability of social engineering assaults while an alternate premise (H_1) posited some employees are far more susceptible to targeting roles. The study also ascertained if there was a serious relationship spanning the attack category (like phishing, vishing, or pretexting) and the information sought, like personal details, account credentials, or financial information. The Chi-Square test gauged these associations, and recapitulated findings in subsequent table 4.4 propose whether particular job roles are more prone to being targeted and whether particular attack categories target certain information.

Table 4. 4: Chi-Square Test Results for Employee Role and Likelihood of Being Targeted

Test Statistics	Value	Degrees of Freedom (df)	p-value
Pearson Chi-Square	53.360	63	0.801
Likelihood Ratio	51.876	-	-
Linear-by-Linear Association	0.352	-	0.553

The Chi-Square test output in Table 4.4 evaluates the association between an employee's job title and his or her chances of being a target for social engineering attacks. The Pearson Chi-Square statistic totals 53.360 possessing 63 degrees of freedom, with 0.801 representing the p-value, which exceeds the conventional importance threshold of 0.05. Consequently the designation of an employee lacks correlation to their likelihood of being victimized to a statistically meaningful degree. Thus, social engineering attacks seem irrespective of role. As it is deficient in both degrees of freedom and a p-value, the Likelihood Ratio cannot be construed in isolation, although presented. The Linear-by-Linear Association test determines if the two variables move proportionally as 0.352 with a p-value of 0.553 which additionally indicates job position plus likelihood of attack share no meaningful linear relationship. These discoveries in their entirety denote workers get targeted without bias irrespective of station, also social engineering methods might be affected via broad organizational factors instead of via job function.

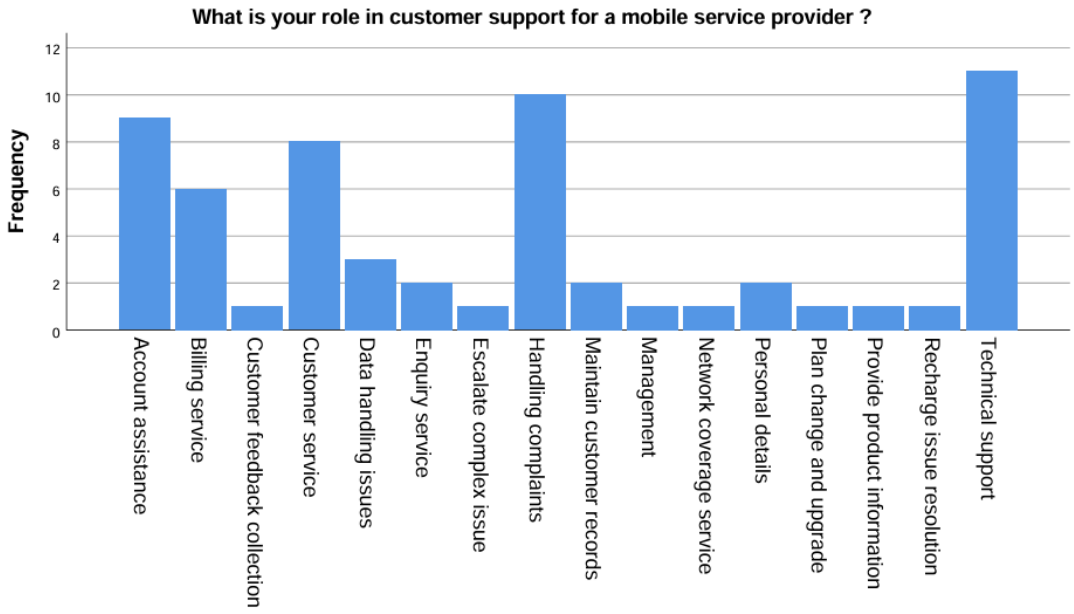

Figure 4.3: Role in Customer Support for a Mobile Service Provider

Figure 4.3 provides a visual representation of the frequency of different roles within customer aid for the mobile service provider. The title is "What is your role in customer aid for mobile service providers?" apparently specifies the intent of the graph. The vertical Y-axis denotes the event's frequency for each role because each time's height indicates how frequently that specific role is documented or witnessed. The horizontal X-axis enumerates functions within customer assistance such as "technical support," "billing service," "handling complaints," "customer service," and several others. Each role possesses an abundance of reactions. The bar within the chart constitutes these numerals, helping to identify which roles in customer aid interactions are the lowest and the least common. One of the most striking comments from the graph is that "technical support" is the most frequently reported role, as indicated by the highest bar. This shows that solving technical issues is a primary function of customer aid in the mobile service provider industry. Given the complexity of problems related to mobile networks, equipment, and software, customers often want troubleshooting, connectivity issues, and assistance with device configuration. As a result, technical support workers play an important role in ensuring customers' satisfaction and service continuity. Another highly popular role is "complaints handling," which has a relatively high frequency. This highlights an integral part of interpersonal interactions rotates to address grievances,

service dissatisfaction, and problem solutions. Similarly, "account aid" also often appears, suggesting that many customers help representative users manage their accounts, such as individual details, updating the billing.

Some roles are less prominent in the chart. Categories like "Management," "Personal Details," "Network Coverage Service," "Plan Change and Upgrade," and "Provide Product Information" show substantially diminished thresholds, implying these positions are less commonly observed during client assistance exchanges. These positions materialize with diminished regularity, suggesting oversight courtesy of designated divisions. Patrons might infrequently require support within these specific domains, too. Network coverage concerns may be handled via automated systems or network monitoring teams rather than customer interaction. Similarly, inquiries on plan changes and product details could be more self-service-based with customers obtaining the information through online platforms or mobile applications instead of customer support. Another keen observation is that functions like "Inquiry Service" and "Escalate Complex Issues" have extremely low thresholds, implying these processes are either exceptional or possibly combined with other functions. The low frequency of inquiry services could imply that customers generally get their answers via FAQs, websites, or automated chatbots rather than contacting customer care for basic questions. Concurrently, the limited reporting of escalation of complicated issues may mean that first-level support agents are solving the majority of issues without requiring higher-level intervention. But this could also point to a possible gap in the management of complicated cases since customers with difficult issues might need more effective escalation procedures.

The findings from this chart imply substantial ramifications for purveyors of cellular service. Initially, one must distribute the resources within locales requiring maximal client assistance. Companies could need to spend further toward enlisting, educating, and employing their support personnel within these locales. Technical support, account support, coupled with complaint resolution are jobs that people report upon most frequently. Customer satisfaction coupled with brand image elevate through a powerful complaint resolution process, while service effectiveness escalates and customer frustration diminishes with technically skilled support personnel. Subsequently, learning and growth initiatives should concentrate on improving the skill of customer support

personnel to address predicaments, remedy challenges, and defuse disputes. As technical support and complaint resolution are common in customer interactions, it will result in better service quality and accelerated turnaround times if the agents have the required skills. Moreover, the lower frequency of inquiry services and the escalation of complex issues may highlight areas needing improvement. Vendors have the capability of refining self-assistance resources such as AI-supported digital assistants. Thorough online help centers and interactive customer portals would additionally diminish dependence upon live support for basic inquiries. Parallel to this, improving the process of escalation for complex cases can help ensure that customers with outstanding issues are provided with effective and timely solutions without extra frustration. The rarity of network coverage service support may mean customers either do not report issues frequently or that businesses already have good automated detection and resolution mechanisms. Regardless, it is still important to give customers effective channels of communication for network-related issues to ensure reliability in services.

The diagram illustrates the roles in customer support for a mobile service provider. It can be seen that technical support, complaint handling, and account assistance are the main functions. This analysis suggests that a mobile service provider should give priority to these activities, as they are the most in-demand. The provider should also try to make the less common roles more efficient. By streamlining customer support, increasing staff training, and making better use of technology, a mobile service provider can provide better customer service and save money.

Objective 3: Assessing Security Measures and Their Effectiveness

The aim of the third objective is to assess if the availability of safety measures in the organization and the availability of reporting have impacted significantly in decreasing the number of social engineering attacks. This aim was conceptualized using a zero hypothesis (H_0) that read no important correlation exists between the presence of security protocols and the incidence of social engineering attacks, while the alternative hypothesis (H) postulated that instances of social engineering attempts are diminished by strong security protocols plus proactive incident reporting. The research centered on ascertaining if two-factor authentication, employee training on a regular basis, data safety procedures, and the adoption of controls such as transparent event reporting

channels could minimize attack frequency. An analysis into if encouraging staff notification regarding aberrant conduct or possible data compromises might diminish the efficacy concerning social manipulation incursions transpired. We executed a Chi-Square test so we could determine if the tables shown below had statistically meaningful correlation. We scrutinized correlation among safety measures occurring, events reporting, also low attacks strengthening via aggregate results.

Table 4. 5: Chi-Square Test Results for Security Measures and Attack Frequency

Test Statistics	Value	Degrees of Freedom (df)	p-value
Pearson Chi-Square	15.927	3	0.001
Likelihood Ratio	11.407	-	-
Linear-by-Linear Association	1.030	-	0.310
Minimum Expected Count	0.50	-	-

Table 4.5 shows the Chi-Square test results evaluating how security protocols instituted correlate with the tally of social engineering attacks. The Pearson Chi-Square statistic including 3 degrees of freedom totals 15.927. Since the p-value of 0.001 is below 0.05, importance exists ($p < 0.05$). This evinces a tight connection between security controls and frequency of attacks since the type or quantity of security controls impacts the frequency of social engineering attacks. Likelihood Ratio is furnished although it lacks degrees of freedom and any p-value. Attributable to this, Likelihood Ratio becomes less lucid herein. The Linear-by-Linear Association test, which assesses the potential tendency of security protocols versus attack frequency, shows a value equal to 1.030 including a p-value equal to 0.310 because it exhibits no explicit linear tendency amongst the variables. That the data's distribution is acceptable for compliance within the Chi-Square test's stipulations corroborates the 0.50 minimal count anticipated. Organizations should strengthen security protocols for minimizing attack frequency, as

the high Pearson Chi-Square value generally suggests security protocols' effectiveness has a vital role preventing social engineering attacks. The p-value safety processes of 0.001 indicate a strong significant relationship between the presence of safety processes and lack of social engineering efforts.

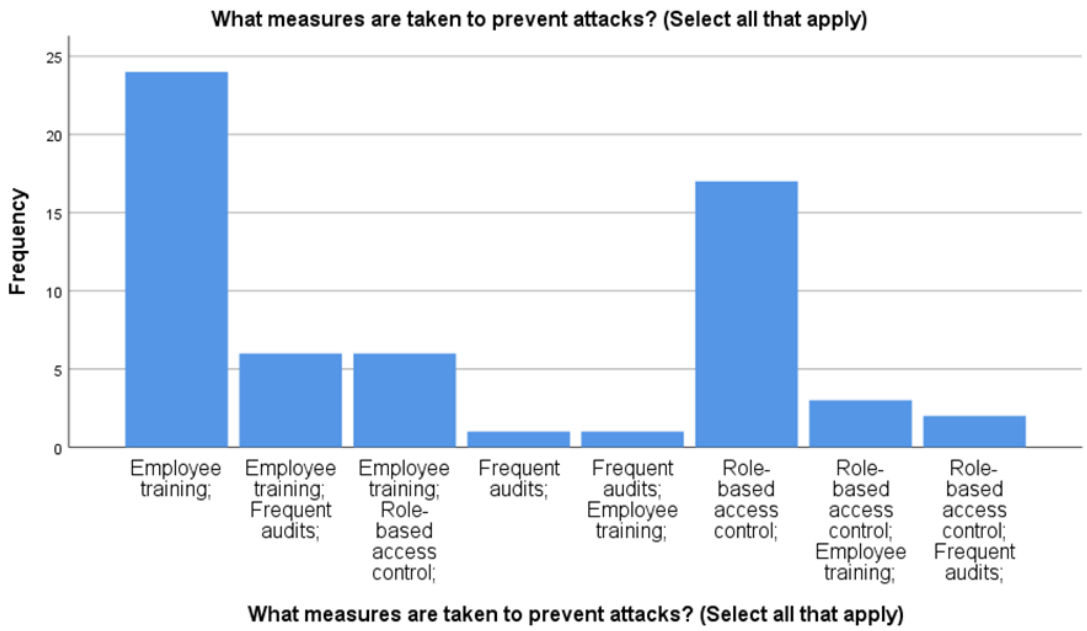

Figure 4. 4: Measures Taken to Prevent Attacks

Figure 4.4 graph denotes the incidence of employed security protocols for attack prevention that were dependent on many suitable measures opted for in the replies. On the x-axis exist diverse security strategies, be it individually or in combination, such as Employee Training, Frequent Audits, and Role-Based Access Control. The y-axis delineates the frequency of each strategy's choice. The most prominent finding is that Employee Training was the most common employed security countermeasure, top bar indicating firms go out of their way to train workers to ward off security attacks, particularly social engineering attacks. Similarly, Role-Based Access Control was highly rated, meaning limiting access to sensitive data based on roles is a frequently employed method too. The chart additionally denotes that organizations predominantly enact combined preventative strategies as opposed to one sole approach. Employee Training & Frequent Audits and Employee Training & Role-Based Access Control, for example, manifest repeatedly since they reveal that firms prefer to supplement training by

employing other security protocols. However, Frequent Audits alone and Frequent Audits & Employee Training have lower frequencies, which would suggest that audit perhaps is not highly viewed as a powerful singular practice but rather as an additive security practice. Moreover, combinations such as Role-Based Access Control & Frequent Audits and Role-Based Access Control & Employee Training are less common, so while access control is necessary, it will be used alone more often than in conjunction with other methods. The low hurdles for other combinations of security measures suggest that some businesses are not employing their security measures whole, which could form gaps in their systems of protection. The findings show that Employee Training and Role-Based Access Control are the most preferred security procedures. Yet, firms must take a yet more overarching stance in how they balance training, access control, and auditing for successful reinforcement of their defensive mechanisms against breach.

This finding validates that corporations instituted strict security policies such as workforce education, credential validation, two-factor authorization, and experienced a noticeable deficiency in social engineering attacks. Similarly, the Chi-Square Test produced the following results for the frequency of incident reporting and attack:

Table 4. 6: Chi-Square Test Results for Incident Reporting and Attack Frequency

Test Statistics	Value	Degrees of Freedom (df)	p-value
Pearson Chi-Square	19.931	6	0.003
Likelihood Ratio	23.911	-	-

Table 4.6 below gives the results of the Chi-Square test of the association between attack frequency and incident reporting. Considering a p-value at 0.003 that is beneath the 0.05 importance threshold, the Pearson Chi-Square amount of 19.931 on 6 df indicates a statistically important correlation. This implies that attack frequency has a significant influence on the probability of incident reporting. The Likelihood Ratio value of 23.911 is strong evidence in favor of the association and supports that differing attack frequency

affects the frequency at which incidents are reported. These findings suggest that higher attack frequency would lead to organizations being more likely to report security incidents, while a low attack frequency would cause incidents to be underreported. This supports the urgency of having active reporting procedures to guarantee that even rare incidents are reported and dealt with efficiently. The P-value of 0.003 reflects a strong correlation between reporting and a decrease in social engineering efforts. Institutions that encourage workforce members in reporting of the episode skillfully curtail their susceptibility for social manipulation incursions.

4.4 Discussion

The objective for this investigation was toward verification of a connection amid worker labor functions. Social engineering attacks bear upon employees, the Chi-Square test of independence looked at this correlation and demonstrated none. This shows that the type of attack received by an employee is not at all determined by the role in which he works. One possible reason for this non-significant finding is that social engineering attacks target human vulnerabilities over job roles. Attackers can apply phishing, pretexting, or baiting methods in any role, attacking employees randomly rather than targeting those dealing with sensitive information or customer interaction exclusively. A further consideration may be security policies within the company that protect against exposure to security threats on a similar level for different job positions, diminishing any specific attack pattern of targeting.

Furthermore, the risk across various employee roles could have been neutralized via training along with awareness initiatives undertaken within the organization. Furthermore, even more reliable offense schemas could have materialized in the event that occurred. If similar security training is provided to employees of different job functions, they can exhibit similar awareness and response mechanisms, thus decreasing substantial variations in attack targeting. Although this finding suggests that no particular role is disproportionately impacted by a particular type of attack, it does not mean that security protocols should be eased. Rather, this result underscores the value of thorough security training for all job functions rather than concentrating on high-risk roles. Subsequent studies may examine other variables—like individual levels of

cybersecurity awareness, history of attack, or departmental security culture—to better grasp the social engineering threat in various workplace settings.

The results provide intricate observations of the association between positions and degrees of vulnerability to cyber-attacks and the efficacy of deployed security. The research reveals that although specific security controls like two-factor authentication and access control are significant factors in minimizing attack frequency, training of employees is the most widely used preventive practice. The role frequency distribution indicates that technical support and account assistance are paramount, so someone likely targets them in social engineering endeavors. In opposition to expectations, employees interacting with customers may not observe more pointed attacks. Statistical analysis reveals no correlation connecting an employee's role to the specific attack experienced. This indicates that social engineering attacks are not specifically role-based but are taking advantage of general organizational weaknesses. Also, though the probabilities of being attacked did not significantly differ across roles, having security measures had a significant correlation with attack frequency, highlighting the significance of organized cybersecurity protocols. The incident reporting analysis further stresses that proactively protecting systems counts since reporting rapidly may avert menaces before they turn unmanageable. Certain assessments demonstrated statistical importance yet others did not. This modification stresses cybersecurity hazard intricacy with the multidimensional protection required. Cybersecurity preventive measures plus awareness must be integrated within all employee functions instead of targeted job roles because overall results validate the theoretical basis. The results agree alongside present investigation on cybersecurity perils throughout customer support contexts, also the results summon active security guidance coupled with policy application. The research definitively highlights the value of organizations with an integrated security tactic combining tech solutions and human awareness programs to combat social engineering attacks.

4.5 Summary

Pinpointing broad social engineering assaults, pinpointed information, coupled with employee positions most vulnerable to such assaults, also appraising the impacts of

security protocols and occurrences to curtail the prevalence of assaults were the focus of the detailed analysis of conclusions based on data collected from employees in customer support roles within mobile service provider organizations in this chapter. Descriptive analysis showed that individual details (35%), account details (10%), and financial information (1.7%) were the most targeted information, while technical support (18.3%), account assistance (15%), and customer service (13.3%) were among the most exposed employee roles. The hypothesis test using the curry tests showed that researchers noticed no important correlation between the employee roles and the type of attack (p-money = 0.993). They found no meaningful association between the type of attack and the target information, suggesting that attackers usually target any accessible information regardless of the employee's role. A strong meaningful relationship (p-mal = 0.001) was discovered nonetheless in reference to safety measures. This correlation involved the existence of meager assault. These discoveries stress that we must diminish the effects of social engineering schemes, of employee education, as well as stringent data security guidelines. This is accompanied by the fact that we must spotlight the effects of sensitive customer details, that we must assess protection.

Chapter 5

Conclusion and Recommendation

5.1 Key Findings

This chapter furnishes a thorough summation since it scrutinizes the data detailed in the prior chapter, which accentuates the key perceptions scholars derived from inquiries concerning social engineering breaches throughout mobile service provider organizations. The study's central objective involved ascertaining the nature of specific data vulnerable to incursions. Of equal importance existed the sway of security protocols along with incident reporting because they curtail the frequency of social engineering attacks. Descriptive analysis has shown that most targeted information by social engineering attackers includes individual details (35%), account credentials (10%), and financial information (1.7%). This shows that sensitive customer information remains the primary target for the attackers regardless of the status of the employee. Additionally, analysis showed that employees working in technical support (18.3%), account assistance (15%), and customer service (13.3%) roles face a high risk for social engineering efforts due to direct access to customer information.

The hypothesis testing gave valuable understanding into how employee roles with targeted information with safety measures reduced social engineering attacks. The initial supposition pertained to the category of social manipulation intrusion. Employee functions underwent assessment regarding their effect on it. Since the Chi-Square Test presented a P-Value amounting to 0.993, the test does not denote substantive correlation between an employee's role and attack type. This implies that attackers do not target a specific job but seek to exploit any employee who possesses access to customer information. The subsequent premise explored if certain staff were likelier to be singled out and if perpetrators correlated assault patterns and victim specifics. The test outcomes showed a P-value of 0.221 and 0.801, respectively, confirming that no particular job role was weaker than others, and the attackers targeted any available information. However, the third hypothesis tested the safety measures and the effect of reporting the incident on reducing social engineering attacks. The Chi-Square Testing yielded a strong meaningful correlation among the presence of strong security protocols,

active event reporting, and low attack frequency for safety measures. The p-value as well as event reporting registered at 0.001 for safety measures. Open culture programs for reporting combined with open cultural awareness of events lead to fewer successful social engineering attacks.

The research ascertains that mobile service provider organizations undergo attacks through social engineering mainly to obtain private information yet attackers do not restrict their activities by occupational role. Entities that institute security guidelines, vigorously defend information, and solicit incident reporting documentation diminish the incidence of social engineering attacks. Comprehensive security protocols coupled with employee education are requisite in preventing social engineering attacks of mobile service providers. Organizational consciousness regarding reporting occurrences is furthermore required. The research results provide essential knowledge that mobile service providers need to enhance their organizational security framework and lower information vulnerability to achieve stronger data defense systems.

5.2 Recommendations

This study provides mobile service provider organizations with practical recommendations to lower their exposure to social engineering attacks and protect sensitive customer data while building a stronger data security system.

5.2.1 Implement Strong Security Measures

A major proposal for the action plan for the mobile service providers to minimize the likelihood and effects of the social engineering attacks, is the incorporation of strict safety measures on all operational levels. Customer details, account numbers, records, and an organization’s data should be shielded from social engineering and unauthorized attempts at accessing the required information. Mobile service providers should adopt better security measures like MFA, password principles, biometric security, and rights access to customers’ data that should be accessible to specific employees. For guaranteeing entry to unapproved and disallowed staff is evaded, workers use MFA. MFA necessitates a minimum of two verifications including social engineering solutions, and the access through unpalatable means to social engineering log-in processes is eliminated.

Besides the user authentication measures, it is recommended that the mobile service provider adopt strong password measures that discourage employees from using hard or easily guessable passwords. They should not use the same passwords in different places and should change their passwords often. This can assist in minimizing the probability of somebody who gets unauthorized access to the system due to credibility by theft. Besides, other protective measurements such as face recognition, fingerprint scan and incorporating voice recognition for higher level security are also effective towards enhancing organizational data safeguarding. Biometric security proves to be an identifier that cannot be imitated by the attackers; hence, fraud cases are minimized.

Another factor of strong safety measures is the policies that specify possible users' access to customers' information to correlate it with their positions at the company. With the use of role-based access control (RBAC), only certain categories of employees can access certain data for instance customer account details and his or her financial and billing information thus reducing the issue of unauthorized personnel accessing or modifying the information as they wish. This remedy greatly decreases the odds of social engineering incidents aimed at the ordinary employees that are not privileged to the admin accounts. Overall, data interception should be prevented and if the data leaked, then the data intercepted should not be intelligible or readable without a decryption key.

Cellular network corporations must further warrant the deployment of a firewall defense protocol. The system should monitor along with regulating the traffic stream inside the networks contingent on safety policies. For an IT manager, firewall is very important to the organization because it acts as barrier that analyses and restricts the incoming and outgoing traffic. Thus, it bars any unauthorized traffic and any other form of activities that might harm the organization's customers and their information. The engagement of infiltration and prevention systems (IPs) on the other hand, enable systems to inspect the status of network traffic in real term, detect as well as bar the invalid efforts to gain entrance automatically other than human caused. It also enables the detection of social engineering attacks.

Nevertheless, there is a belief that the mobile service provider must periodically evaluate the security and perform penetration tests to find out the vulnerabilities and loopholes that attackers can utilize. The assessment involves the scanning of the organization's IT

structure, network system, databases as well as the applications which the attackers would use to identify safety loopholes, misconceptions or weak passwords. On the other hand, penetration tests involve the measures and scenarios used to mimic the safety measures and a fake attack to check on how the event response team responds to the time taken. By conducting these regular assessments, mobile service providers can identify and address potential security weaknesses, reducing the possibility of successful social engineering attacks.

In addition, encrypted data storage must be applied to protect customer data from misuse in case of a data breach. End-to-end encryption ensures that the data is secured during the transfer between two systems, preventing the interception of a third party. Information concerning REST (data stored in the database or server) also must be encrypted through employing 256-bit encryption methods otherwise advanced encryption standard (AES), which renders data's use plus misuse extraordinarily challenging, even upon a violation. This will further enhance the privacy, integrity, and availability of customer data.

Finally, mobile service providers should install a data backup and disaster recovery system to verify that important customer data has been backed up and can be restored quickly in cyber-humiliation or data violation conditions. Consistent data backups curtail data depletion, afford rapid restoration alternatives, plus they guarantee enterprise perseverance should social engineering attacks happen. In addition, the company should implement a network partition strategy, where important systems and databases are separated from the outer network. If an employee's system is compromised through a social engineering strategy, the data reduces the possibility of exposure.

5.2.2 Regular Employee Training and Awareness Programs

Exploitation of human fallibility is the primary avenue for social engineering attacks so recurrent personnel education initiatives remain requisite. These programs heighten cognizance, attentiveness, and furnish personnel with the understanding and adeptness needed to discern and avert fraud attacks. Social engineering attackers often manipulate employees through psychological strategies, assuring them to disclose sensitive customer information, provide unauthorised access, or compromise tasks with the

organizational security. Therefore, extensive and continuous training must be applied to educate employees to identify, escape, and report the dangers of social engineering.

One of the primary areas of employee training should focus on identifying the social engineering strategy, including phishing emails, phishing calls, pretexting landscapes, and copying fraud. Employees should be trained to identify phishing efforts, which often include login credentials, financial descriptions, or emails that replicate the reliable institutions requesting customer information. These training programs should include examples of the real world of phishing emails, highlighting suspected sender addresses, immediate requests, grammatical errors, and general indicators such as malicious attachments or links. Additionally, employees must be taught to verify email authenticity before clicking on the link or downloading the attachment, significantly reducing the possibility of falling for phishing plans.

The same should apply to the wishing (voice fishing) calls, which is when attackers imitate and trick the employees to reveal information to clients, technical support, or corporate executives. Before disclosing any customers' information, account credentials, or other internal company data to the caller, employees should be told to check the identity of the caller through appropriate channels. They should train regarding comprehension of pretexting as a social engineering strategy. A perpetrator defrauds staff within the firm to amass data throughout the fabrication of illusory circumstances. Employees answering information solicitations must be circumspect especially when unforeseen execution proclaims an urgent entitlement.

Another requirement of security awareness entails letting the employees understand that they are prohibited from communicating information belonging to customers without prior approval. Their certification procedures within the company must be followed and one of these include confirming the identity of the customer before divulging any information regarding an account. Moreover, training should point out that in no case should confidential information about customers be disclosed to third parties via unprotected electronic media such as personal emails, social networks, or unauthorized third-party web-sites. To minimize the resultant forbidden disclosures, one can educate the employees so they function under the principle of least necessary access that is they obtain also divulge only as much information as their duties may

require. To safeguard against such menaces and ascertain worker vigilance, social engineering incursions should be enacted periodically as a prophylactic action. organizations are able to execute test phishing, as an instance, for comprehension of employee reactions. It is vital to ascertain how employees react toward such emails. Additional instruction shall be furnished to personnel incapable of discerning the artifice, while security specialists for other staff members will be people who succeeded. Workers may likewise execute desires and pretexting assaults wherein diverse scenarios are feigned for building cogitative skills with apt real-world response methods.

A good employee training program should also entail a strong focus on reporting any insecure activities and enhancing security awareness and concerns to the IT security department or management. The employees should be advised to alert the management of any strange emails, phone calls or customer requirement that may be fake. There should be a good and well-understood process in writing the event reports, and they should understand what to do when in contact and when there is the possibility of social engineering attempts. Permits organizations to establish specific reporting means, for example, hotlines, informational-only e-mails, and internal threat boards, concerning safety dangers. Thirdly, it is particularly crucial for an organization to have an organizational culture that discourages social engineers from being successful in their attempt. Regulations must be able to present that each employee should contribute toward protection of data as well as customer information. It suggests everyone bears accountability regarding cybersecurity. For the company's protection from social engineering threats, it should ensure constantly updated cybersecurity enlightens staff via newsletters, posters, workshops, and team discourses. Hence, organizations should consider their human element by identifying the staff and ensuring that it is trained to recognise social engineering techniques and promptly report them, towards a secure organizational culture in every sector.

5.2.3 Encourage Incident Reporting and Response Mechanisms

This study also revealed the relationship linking submissions to lessen assault occurrences and validated that the active event reporting could help to mitigate social engineering attacks. Therefore, the institutions must enact suitable procedural chains in instances of questionable happenings. This implementation will ease prompt reporting.

The management needs to come up with a way of dealing with the reported events to ensure these activities are dealt with promptly to avoid instances of violating the data.

5.2.4 Limit Employee Access to Sensitive Information

The research also indicated that people in technical support, accounting assistance and more specifically, consumer services are most vulnerable to face social engineering attacks. Accordingly, RBAC's enactment remains vital because it governs permission. Hence, field support personnel need to procure data applicable to their functional obligations. This is true as the flow of extremely sensitive information can be restricted to reduce the risks of information violation and the consequences of social engineering attacks.

5.2.5 Conduct Regular Security Audits and Vulnerability Assessments

In that regard, one of the most reliable measures to mitigate the threat of social engineering attacks and protect the data in mobile service provider organizations is security audit, regular assessment of potential vulnerabilities, and constant completion of entry tests. They involve; These are key in revealing compromising vulnerabilities and misrepresentations of a system security, which the social engineering attackers use to gain access into confidential data belonging to the customers. About performing security audit and vulnerability assessment it can be stated that regular security audit and risk analysis helps an organization to improve safety & security system, minimizes risks and lower probability of social engineering attacks. Hence, it is suggested that mobile service purveyors examine safeguards plus evaluate frailties exhaustively either each quarter or biannually to guarantee their data protection architecture stays current, conforming, and adaptable when facing emerging social manipulation menaces. Conversely, a protection review might be characterized as a wide-ranging investigation of a firm’s data network. The policies and structures around it are likewise scrutinized for ascertaining its adherence toward safety standards plus for evaluating its protection capability versus an intruder, a data violation, and social engineering. The primary purpose of a safety audit aims to determine safety intervals, misunderstanding systems, unauthorized data access, and human errors that can potentially highlight customers' information for social engineering hazards. During a safety audit, organizations review employee behavior, data handling procedures, access control measures, password management, and

communication protocols, which can help exploit the attackers to detect any weak points. For example, if the audit is identity.

From the above findings, it is evident that the most efficient practice to combat the social engineering attacks and protect the data in mobile service provider organizations is through the conduct of safety audits, vulnerability evaluation, and entry tests frequently. These processes are of paramount importance in recognizing possible security threat, comprehending general concept of security vulnerabilities and misperception, where social engineering attackers may take advantage of to penetrating customer information systems. Safety audits and annually completed vulnerability evaluations can help fortify the safety systems of an organization, decrease various threats, and minimize actuality of planned social engineering. Hence, it is wise for mobile service providers to routinely examine security plus evaluate susceptibility each quarter or semester. This confirms the enterprise's data security architecture remains current, compliant, and adaptable regarding potential infrastructure social engineering. A safety audit can be defined as the method of assessing info system, security policies and structures in an organization to check whether they give adequate protection against safety threats such as unauthorized access, data breach, and social engineering threats. Thus, a safety audit's principal objective constitutes identifying safety lapses, misunderstandings, forbidden data access, coupled with human errors. These matters may lead to customer data being regarded as part of a social engineering menace. Throughout the safety audit, the attackers are able to observe employee operations, business process specimens whereby data collection and processing occurs, methods for entrusting data access, password policy, and communication procedures because of their availability.

For instance, a penetration examiner may try to perform a phishing email attack on the customer service employees or may call the executive of a company through vishing and gain information of the customer account. In case the penetration test is successful, it can be followed by improvements in the organizational safety measures, staff awareness, and controlling the access to the organizational network and information. For the same reason whenever securities are changed frequently, or there are alterations in the structure of organizations procedures, or maybe due to changes in security laws or issues such as cybersecurity threats. It is helpful for the organizations to conduct

quarterly or semi-annual security audits. The Data Protection Directive along with the Data Security Act represented particular statutory obligations germane to the mobile service provider domain, principally the GDPR and the Telecom Consumer Protection Regulations that require firms to safeguard customers' information from theft, and cyber incidents. Thus, when facing security audits, the organizations can increase the compliance of their safety policies, customer data security standards, and event response plans with the norms of the current legislation to minimize the possibilities of legal sanctions and reputational loss. In addition, these audits make it easy to create trust with the customers as they know their details such as their account details, payments, and any other personal information they have provided to the company are safe from third-party tampering.

Another advantage of performing regular safety audit and vulnerability assessment is increased effectiveness when developing the event response plans. Information acquired from the analysis of the previous attack of social engineering can help organizations realize the common areas of vulnerability exploited by the attackers, and then draw up specific protection measures to counter such incidents. For instance, if the previous social engineering attacks were in the form of emails, the organization can develop measures such as email filtering, verify email identity and train the employees to avoid using emails that may contain such phishing attacks. Likewise, if the organization establishes that the psychic customer service wishing calls were a problem, then the caller identification verifications may be instituted. Multitiered credentials might additionally curtail the transmission of deceptive information. Furthermore, mobile service providers must employ outside service Integrators, suppliers, and allies for their security audit or vulnerability check to significantly reduce the likelihood of supply chain security threats. The impunity of the attackers is to infiltrate the infrastructure of the primary organization with the help of third-party vendors and access customer data. Thus, third party vendors must be compelled to adhere to certain data security policies, safety audit measures and procedures as well as measures to mitigate vulnerabilities within the entire organizational network. This is to enhance protection of networks employed by mobile service providers.

Contemporaneous data surveillance systems are likewise advocated since networks, databases, plus communication channels are routinely scrutinized to detect illicit operations. Security information and event management (SIEM) system can assist to determine the notable activities, attempt of data violation, and unauthorized access intending to exist in real time. Such monitoring systems cause alarms when they discern some social engineering scheme, and they let the security team to follow and prevent the formation of the information agreement. Last but not the least, it is also advisable for the mobile service providers to adopt certain measures like regular safety audits, vulnerability assessments, and conducting admission tests as the ways to address the SE attacks. This includes safeguarding customers' information and safety compliance on an ongoing basis. In essence, an organization has the capacity of minimising its vulnerability to social engineering attempts through eliminating the security risks and confusion as well as undermining the system. Besides, compliance with regulatory requirements, extending the event response protocol and proper data access control makes it possible to enhance the organization's defence against social engineering attacks. Consequently, mobile service vendors should implement a periodic security assessment every three or six months, as well as vulnerability and entry test in an effort to boost their data security efforts, minimise on human error flaws and gain customer trust.

5.2.6 Establish a Data Protection and Privacy Policy

First, an effective data security and privacy policy (DPPP) constitutes an important prerequisite toward organizational security of mobile service providers and customers' information against social engineering attacks. This directive functions as a structured framework, and it delineates processes, conventions, and benchmarks. For ensuring maximum data security, it processes, saves, and accesses sensitive customer information. The rationale for escalating the data security and privacy policy goals is to safeguard the customer information, curb unlawful access by third parties and operate in legal compliance to the handling of personal information. The mobile service provider can benefit from the above plan by being able to control the onslaught of social engineering attacks, data violations, and unauthorized data access over the customer data. This data should stay confidential, safe, and protected at all times. A Data Security

and Privacy Policy (DPPP) represents a compendium of directives and stipulations, and it addresses how people govern consumer details including instruction on accessing data, managing received data, handling deficient data, and shielding it from illicit access and tampering. The policy should be cognizant of customer information specifics including account information, personal information, payment information, plus usage records concerning the service. Generally, the functional application of this data must be permitted for credentialed people alone. An additional vital directive needs focus upon gateway regulations as such regulations must confine admission for all customer specifics solely toward assistance personnel, invoicing, plus account managers. This Role-Based Access Control (RBAC) minimises the likelihood of cases whereby unauthorized people access various information and offers protection against social engineering attacks.

Data security as well as privacy policy should, furthermore, delineate the legal along with moral sanctions applicable to information infringement. Employees should be fully informed as well as trained regarding disclosing customer information's legal consequences, whether unknowingly or else intentionally. Any worker who sends private data or customer account details with those not allowed should have this policy make that clear (either phishing emails, wish calls, or through pretexting efforts) will face strict disciplinary action, including employment, legal action, and financial punishment. Such rigid compliance frustrates workers when managers ignore details, thus reducing any risk that hackers manage attacks. About data encryption data protection and privacy policy should speak. Data storage practices that are safe are also of great importance. To guarantee that it is invulnerable, all client data, be it concrete documents, cloud repositories, or in electronic form, should be encoded via advanced encryption standards (AES-256 or higher) so it remains inaccessible without an authorized decryption key. Furthermore, the policy should render frequent data backup compulsory for diminishing the forfeiture of clients' details. It shall curtail losses involving data breaches, cyber-attacks, or infrastructure failure too. For guaranteeing customer data is restored with haste throughout a data breach or network anomaly, its periodic backup must be kept within a discrete, secure locale, which curtails social engineering assault repercussions.

Data security and privacy policy should also be given strict punishment for noncompliance with data safety standards. It is particularly crucial to note any employee, third-party vendor, or external stakeholder negligent or noncompliant with data security policy will face immediate disciplinary functions, including legal consequences and financial punishment. For instance, if a customer service employee voluntarily or carelessly shares count details or finimportantancial information without proper verification protocol, they should abolish employment or legal action according to the policy. Similarly, third-party vendors or service providers who handle customer data (e.g., billing services, cloud storage providers, or software vendors) must be required to follow data safety and privacy policies to safeguard against data leaks, misuse of information, or unauthorised access. This third-party compliance requirement is important, as the attackers often target external vendors to achieve access to customer information indirectly.

In addition, the policy must install clear data retention and disposal processes to prevent long-term data exposure. Customer information that is no longer necessary for commercial purposes plus data exposure should be safely disposed of or removed from the company's database for the reduction of exposure risks. Data settlement policy should define specific procedures for safely removing digital data through safe erasure software. Document shredding should also prevent data violations that improperly renounced records cause. Furthermore, the policy must require frequent auditing and analysis of data storage practices to make certain they store only necessary customer information and then immediately deal with fruitless data.

Another key aspect of the data protection and privacy policy is that the company follows national and international rules that regulate data protection such as the General Data Protection Regulation (GDPR), the Data Protection Act (DPA) or other industry regulations. Such rules help to abide with the country’s legal provisions on customer data privacy, data security, and consumer rights security. Besides the concerns mentioned above, the policy simply needs to require more frequent internal scans and vulnerability tests to protect against the ever-rising threats of social engineering.

To aid enforcement of the data security policy, personnel should be tutored within privacy implementation programs plus within safety awareness and data security. With

frequent instruction including private details plus consumer records, staff will comprehend accountabilities within information safeguarding. They must also comprehend social engineering attacks as well as phishing emails. Via phishing calls, these attacks coupled with emails may induce the customers for provision of the information. By the policy, employees should further be required to report suspicious activities. Data violations and unauthorised access efforts should be reported by you to either the IT Safety Department or the Data Safety Officer (DPO). A clear reporting channel lets the organization act appropriately on data violations. This action allows the organization to identify risks and to limit ramifications from social engineering intrusions.

Also, the policy on data protection and privacy shall apply to third-party contractors, agents, and other parties from the mobile service provider who collect, process, store or otherwise deal with the customer data. Many organizations have ties with third-party entities such as cloud service providers, payment processors, or software vendors who are in possession of privilege information of their customers and hence pose possible threats for social engineering. That is why by defining the working relationships with third-party contractors, the policy has to include the requirement of IT security compliance that covers data encryption/decryption, multi-factor authentication, and the restriction of data access. Each and every act of failing to maintain among third-party vendors and clients' data safety measures should warrant termination, legal prosecution, or otherwise a financial loss to act as reinforcement for data protection to be put in place strictly.

Last but not least, it becomes crucial to conclude that general 'Data Protection and Privacy' policy (DPP) should be implemented in the environment of mobile service providers for the sake of customers' data confidentiality and avoiding potential data violation incidents. This also includes obvious reduction of the success rate for the social engineering attacks' occurrence. Mobile service providers define the processes for handling data. They also set up the access control measures, set up data encryption standards, make third-party compliance compulsory, in addition to thus safeguarding customer information since forbidden entities may access customer data, leak data, and exploit social engineering. Moreover, the procedure for punishment for non-con- non-non-non-non-non-non-non-non-non-non-non-non-transportation, makes the employees

aware of legal consequences, moral values and risks pertaining to data violations, which will minimize the organization's risks of being affected by social engineering. This policy will enhance customer data protection, contribute towards organizational improvement of their image, help in building customer confidence, and meet legal requirements. Observance of data protection and privacy policy in conjunction with rigid application of client data will act as a formidable barrier. Eventually, this should considerably curb the prevalence besides impacts from social engineering scams plus information privacy.

5.2.7 Promote a Strong Cybersecurity Culture

Overall, it may be implied that sustaining a healthy cybersecurity culture among the MSP within a mobile service provider organization is an effective and proactive way of managing social engineering attacks. A cybersecurity-orientated organizational culture emphasises the importance of collective responsibility in protecting customers' information from fraudulent activities and social engineering attacks. When employees internalise the cybersecurity values and adopt the security-essential mentality, they are actively involved in customer data protection, potential threats, and reported suspicious activities, reducing the success rate of social engineering attacks. Accordingly, cultivation of a cybercity-conscious organizational ethos has importance to strengthen organizational flexibility facing social engineering threats because it assures the safety and privacy of customers.

A strong cybersecurity culture begins with the leadership team of the culture organization that promotes safety approaches that prefer data security and safety practices in every aspect of professional operations. The executive staff should articulate precisely why cybersecurity is meaningful to them. Every worker should comprehend his or her function. They must be responsible as well for safeguarding customers' information. By integrating data security as a main value, employees will develop a natural vigilance towards potential social engineering attacks, making them capable of identifying, preventing, and reporting any suspicious activities. For instance, should an employee appeal to a patron or superior and then obtain a fraudulent email, a cybersecurity-managed culture will motivate the employee to immediately report the incident to the IT security team instead of being an attack. This collective, safety-

conscious behaviour significantly reduces the risk of data violations caused by human error.

To strengthen cybersecurity culture, mobile service providers should create systems that allow customers to actively protect customer information. These programs should include interactive training sessions and workshops together with role-practicing exercises. In these exercises, the landscapes of real-world social engineering attacks should be simulated via phishing emails, wish calls, presence, and copy efforts. It is also necessary to convey to the employees how to recognize such things as phishing mails, arbitrary offers to require more details from clients, and attempts to gain unauthorized access. It also needs to include a disclosure of the customer information to third parties without any form of verification and proper standard operating procedures when handling of sensitive data. Safety training keeps the employee knowledgeable in that it makes everyone conform, so it is improving the employee's security to social engineering attacks which is set within the organization.

One of the important methods for cultivating an effective cybersecurity culture is to ease the employees reporting incidents absent apprehension of retribution for doing that. Social engineering incursions function a prominent amount of instances since personnel do not report to the organization’s supervision because they do not prefer culpability or discipline. Thus, cellular network corporations must espouse an unsophisticated disclosure ethos. Consequently, the personnel can divulge possible social engineering menaces including phishing emails, disallowed endeavors, also pretexting environments. organizations must institute reporting systems germane to event reporting. Employees can ensure reporting that is swift and facile through hotlines, safety dashboards or email reporting when they come upon suspect actions in lieu of a typical system. Also, the organization needs to consider providing the means of reporting cases of social engineering by employees without subsequent persecution which would foster the high level of employee vigilance.

It also entails acknowledging and promoting the electronic security-conscious employees who would help to prevent such social engineering attacks. For example, when an employee notices and reports a phishing email, or phishing voice call or someone within the organization seeking to rip off the company, the organization ought

to laud the conduct. It does not only ensure positive cybersecurity attitude but also creates awareness to urge the rest of the employees to ensure they protect the customers information. Also, the mobile service providers may bring other motivative cybersecurity activities like monthly cybersecurity heroes, data guards or bonuses for the staff who implement high level of data security. This strategy encourages people to adopt the safety culture as part of organizational goal and everyone is expected to contribute to the protection of customer information.

Another crucial element to advance the notion and practice of cybersecurity culture is to maintain guidelines on cyber safety in the organization's day-to-day business operation and functions. This includes the following elements of information technology security best practices: strict approach to data access rights multi-factor authentication (MFA), data backup at specific intervals, and frequent vulnerability scans. For instance, the moment that the employees are checking the information of the customers, the system should be programmed to ask for a second password to prevent unlawful entrance. Furthermore, the internal communication methods of the organization must be monitored in order not to receive phishing emails, unapproved downloads or any other form of suspicious activity possibly involving file transfer. Systemic security culturing also means that information security becomes a regular working process for employees, and they are aware of potential threats and involved in customers' data security.

Second, developing an employee-IT security team collaborative cybersecurity culture is also a prerequisite to preventing social engineering attacks. The employees need to feel safe in reporting suspected data breaches or suspicious activity to the security team. The IT security team should then react in real time while updating security alongside technically assisting employees so that the organization may respond quickly to any social engineering attempt. The collaboration is a robust in-house defence system, where the employees are the first line of defence while the IT security team carries out technical control. The culmination is a wide-ranging, multidimensional security architecture. It diminishes the success rate within social engineering assaults.

Developing a strong cybersecurity culture suggests that you influence external stakeholders, third-party vendors, and service providers to adhere to the organization's data safety practices. Mobile service providers typically depend on third-party vendors

for information storage, payment handling, and cloud services. Social engineering attackers may procure forbidden access toward customer information. They accomplish this via exploiting third-party vendors' weak security practices, though. Accordingly, cellular network firms must guarantee outside suppliers satisfy data protection accords, abide by regulations, and recognize cybersecurity instruction. The company should routinely examine third-party providers' security to ensure their data safeguarding protocols adhere to the institution's safety regulations and curtail the likelihood of secondary social manipulation attempts arising. Mobile service providers should incorporate cybersecurity policies in organizational vision, missions, also operational plans so that data security is a key commercial value. It can be done by creating a cybersecurity charter that specifically communicates the organization's commitment towards the protection of customer information, restricting security threats, and averting social engineering attacks. When cybersecurity becomes a main organizational value, employees naturally adopt safety-conscious behaviours, which increases overall flexibility against social engineering attacks.

Finally, promoting a strong cybersecurity culture in mobile service provider organizations is necessary to protect customers' information, reduce social engineering attacks, and increase overall data security. Employees can significantly reduce the success rate of social engineering attacks by promoting accountability, encouraging event reporting, conducting continuous security training, and rewarding active safety behaviour. Apart from that, stimulating collaborative engagement between employees, security staff, and outsourced vendors will also enhance cybersecurity responsiveness. Lastly, organizational culture development that is cybersecurity-focused will enable mobile service operators to safeguard customer information, build organizational reputation, and restrict the likelihood of data breaches or social engineering attacks.

5.2.8 Future Research Recommendations

Future research can augment the discoveries despite this study affording salient perceptions within social engineering attacks toward mobile service providers:

- Given that social engineering incursions are not confined to a single domain, broadening research parameters to include sectors such as banking, e-

commerce, and healthcare is important. Cybercriminals aim for all of these sectors quite frequently, thus they contend with large quantities of confidential data. Phishing and copy strategies to steal financial credentials are commonly used by the attackers in the banking sector to extract financial information, while fraud tactics in the e-commerce sector manipulate customers into entering payment information. Healthcare organizations maintain wide-ranging volumes of individual medical documentation as well as handle ransomware offenses attributed to identity appropriation. A comprehensive research study encompassing all these sectors will give a clear idea of social engineering threats and differentiate safety measures utilized in sectors.

- An analysis of emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML) and Blockchain could be a source for innovative solutions to counteract the growing threat of social engineering attacks. AI and ML users can avert fraud via analyzing behavior patterns plus spotting discrepancies within those patterns instantly. These techniques can also be employed in automatic phishing detection systems that catch suspicious e-mails prior to delivery to the intended recipient. Having a decentralised and tamper-proof nature, Blockchain can indeed further data security by preventing data abuse and enforcing secure transactions. The current application of these techniques and the exploration of future developments can assist the defence system of an organization against social engineering strategies.
- These comparative studies shall explore just how organizations apply safety measures as they curtail instances of social engineering. This eases the determination of optimal methods. While some organizations may have better employee training, others may depend on advanced cybersecurity tools. A comparison will give researchers insight into what works best for what risk. Also, by knowing the difficulties faced by organizations in applying security, they may help contribute to practical and adjustable solutions for different industries.
- It requires the prevention of events, but also a tendency for events over a period to be reported less and less, which will correspondingly reflect a long-term decline in the success of such attacks. This area would include a scrutiny of the efficacy concerning security policy strengthening, awareness initiatives, together

with active employee instruction. Entities can evaluate the efficacy regarding their safety procedures via gauging lasting patterns within incident documentation. Intruders might be modifying tactics to circumvent those defenses should the protection prove inefficacious. Pinpointing strategies that bring about a steady decline in social engineering incidents would help an organization's continued refinement of its cybersecurity architecture on an ongoing basis.

- Examining the mental elements impacting workers within social engineering exploits is quite vital for encouraging improved protective tactics. Assailants leverage cognitive biases, emotions, and social behaviors. This contrivance causes people to disclose private information. Enterprises can educate their personnel in manipulation detection if they scrutinize how stress, confidence, authority, prejudice, and urgency sway decision-making. Security awareness campaigns benefit from psychological studies. These initiatives find increased acceptance from personnel during advocacy for a safety-aware atmosphere.
- By discovering these aspects in detail, organizations can develop a multidimensional approach to combat technological innovations social engineering, comparative analysis, long-term evaluation, and psychological insights to create a strong cybersecurity structure.

5.3 Summary

This chapter concludes the study about research findings along with objectives identified to tackle social engineering attacks in mobile service provider organizations. Malicious actors will target each employee within the organization, irrespective of that person's role. The nature of assault (P-Value = 0.993) and the staff positions are uncorrelated. However, the findings revealed that organizations with strong safety measures and active event reporting mechanisms have experienced a significant decrease in the intensity of the attack. This has been confirmed by P-Human = 0.003 for the Chi-Square Testing (P-Human = 0.001) and phenomenon reporting for safety measures. Based on these findings, the study advocated regular staff instruction, rigid access regulation, increased organizational elasticity against social engineering offensives, and the advancement of the incident reporting to the multi-factor authentication (MFA). In addition, since staff entree into private details remained restricted, scheduled safeguard examinations

existed, and an explicit data defense protocol stood established, these operations were highlighted as vital procedures for protecting the client's intelligence. For detection of the AI-based hazard, the chapter urged perpetual enhancement of the security infrastructure, real-time surveillance, and routine vulnerability assessment. Subsequent investigation might broaden its purview to additional sectors to discern technology's function regarding managing social engineering assaults. Additionally, it might assess the lasting impacts from worker instruction with notification for diminishing those perils.

References

Adil, M., Khan, R. and Nawaz Ul Ghani, M.A. (2020) 'Preventive Techniques of Phishing Attacks in Networks', in *2020 3rd International Conference on Advancements in Computational Sciences (ICACS)*. *2020 3rd International Conference on Advancements in Computational Sciences (ICACS)*, Lahore, Pakistan: IEEE, pp. 1–8. Available at: https://doi.org/10.1109/ICACS47775.2020.9055943.

Airehrour, D., Vasudevan Nair, N. and Madanian, S. (2018) 'Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model', *Information*, 9(5), p. 110.

Akyeşilmen, N. and Alhosban, A. (2024a) 'Non-technical cyber-attacks and international cybersecurity: the case of social engineering', *Gaziantep University Journal of Social Sciences*, 23(1), pp. 342–360.

Akyeşilmen, N. and Alhosban, A. (2024b) 'Non-technical cyber-attacks and international cybersecurity: the case of social engineering', *Gaziantep University Journal of Social Sciences*, 23(1), pp. 342–360.

Alabdan, R. (2020a) 'Phishing Attacks Survey: Types, Vectors, and Technical Approaches', *Future Internet*, 12(10), p. 168. Available at: https://doi.org/10.3390/fi12100168.

Alabdan, R. (2020b) 'Phishing attacks survey: Types, vectors, and technical approaches', *Future internet*, 12(10), p. 168.

Albladi, S.M. and Weir, G.R.S. (2020) 'Predicting individuals' vulnerability to social engineering in social networks', *Cybersecurity*, 3(1), p. 7. Available at: https://doi.org/10.1186/s42400-020-00047-5.

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

Aldawood, H. and Skinner, G. (2019) 'Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues', *Future Internet*, 11(3), p. 73. Available at: https://doi.org/10.3390/fi11030073.

Alghenaim, M.F. *et al.* (2022) 'Phishing attack types and mitigation: A survey', in *The International Conference on Data Science and Emerging Technologies*. Springer, pp. 131–153.

Aliyu, F. *et al.* (2021) 'Detecting Man-in-the-Middle Attack in Fog Computing for Social Media.', *Computers, Materials & Continua*, 69(1).

Al-Otaibi, A.F. and Alsuwat, E.S. (2020) 'A study on social engineering attacks: Phishing attack', *Int. J. Recent Adv. Multidiscip. Res*, 7(11), pp. 6374–6380.

Alsufyani, A.A. and Alzahrani, S. (2021) 'Social engineering attack detection using machine learning: Text phishing attack', *Indian J. Comput. Sci. Eng*, 12(3), pp. 743–751.

Alzahrani, A. (2020) 'Coronavirus Social Engineering Attacks: Issues and Recommendations', *International Journal of Advanced Computer Science and Applications*, 11(5). Available at: https://doi.org/10.14569/IJACSA.2020.0110523.

An Automated System for Detecting and Preventing Phishing Attempts on Steam Accounts | IEEE Conference Publication | IEEE Xplore (no date). Available at: https://ieeexplore.ieee.org/abstract/document/10389578 (Accessed: 20 February 2024).

Apruzzese, G. *et al.* (2019) 'Addressing Adversarial Attacks Against Security Systems Based on Machine Learning', in *2019 11th International Conference on Cyber Conflict (CyCon). 2019 11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia: IEEE, pp. 1–18. Available at: https://doi.org/10.23919/CYCON.2019.8756865.

Aşan, C. (2023) 'THE ROLE OF CYBER SITUATIONAL AWARENESS OF HUMANS IN SOCIAL ENGINEERING CYBER ATTACKS ON THE MARITIME DOMAIN', 5(2).

Aun, Y. *et al.* (2023) 'Social engineering attack classifications on social media using deep learning', *Comput. Mater. Contin*, 74(3), pp. 4917–4931.

Bakare, B. and Ekolama, S. (2021) 'Preventing man-in-the-middle (MITM) attack of GSM calls', *European Journal of Electrical Engineering and Computer Science*, 5(4), pp. 63–68.

Basit, A. *et al.* (2021) 'A comprehensive survey of AI-enabled phishing attacks detection techniques', *Telecommunication Systems*, 76(1), pp. 139–154. Available at: https://doi.org/10.1007/s11235-020-00733-2.

Bhusal, C.S. (2021) 'Systematic review on social engineering: Hacking by manipulating humans', *Journal of Information Security*, 12, pp. 104–114.

Borowiec, Ł. *et al.* (2023) 'The analysis of social engineering methods in attacks on authentication systems', *Advances in Web Development Journal*, 1, pp. 83–106.

Botta, A. *et al.* (2023) 'Cyber security of robots: A comprehensive survey', *Intelligent Systems with Applications*, 18, p. 200237.

Bullee, J.-W. and Junger, M. (2020) 'How effective are social engineering interventions? A meta-analysis', *Information & Computer Security*, 28(5), pp. 801–830. Available at: https://doi.org/10.1108/ICS-07-2019-0078.

Campobasso, M. and Allodi, L. (2020) 'Impersonation-as-a-service: Characterizing the emerging criminal infrastructure for user impersonation at scale', in *Proceedings of the 2020 ACM SIGSAC conference on computer and communications security*, pp. 1665–1680.

Chebii, P.J. (2021) *Securing Mobile Money Payment and Transfer Applications Against Smishing and Vishing Social Engineering Attacks*. PhD Thesis. University of Nairobi.

Conteh, N. and Schmick, P. (2016) 'Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks', *International Journal of Advanced Computer Research*, 6, pp. 31–38. Available at: https://doi.org/10.19101/IJACR.2016.623006.

Conteh, N.Y. and Schmick, P.J. (2021) 'Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks', in *Ethical hacking techniques and countermeasures for cybercrime prevention*. IGI Global, pp. 19–31.

Das, D. *et al.* (2022) 'Understanding Security Issues in the NFT Ecosystem', in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. CCS '22: 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles CA USA: ACM, pp. 667–681. Available at: https://doi.org/10.1145/3548606.3559342.

Dhake, B. *et al.* (2023) 'A Thorough Comparison of AI-Enabled Phishing Attack Detection Strategies'. Rochester, NY. Available at: https://doi.org/10.2139/ssrn.4422835.

'ED610591.pdf' (no date). Available at: https://files.eric.ed.gov/fulltext/ED610591.pdf (Accessed: 20 February 2024).

Falade, P.V. (2023) 'Decoding the threat landscape: Chatgpt, fraudgpt, and wormgpt in social engineering attacks', arXiv preprint arXiv:2310.05595 [Preprint].

Flores, W.R. and Ekstedt, M. (2016) 'Shaping intention to resist social engineering through transformational leadership, information security culture and awareness', *Computers & security*, 59, pp. 26–44.

Ghafir, I. *et al.* (2018) 'Security threats to critical infrastructure: the human factor', *The Journal of Supercomputing*, 74, pp. 4986–5002.

Gragg, D. (2003) 'A multi-level defense against social engineering', *SANS Reading Room*, 13, pp. 1–21.

Gupta, P., Patil, H.A. and Guido, R.C. (2024) 'Vulnerability issues in automatic speaker verification (asv) systems', *EURASIP Journal on Audio, Speech, and Music Processing*, 2024(1), p. 10.

de GUZMAN, G. (2022) 'NFT marketplace design impact: comprehensive analysis of NFT market and ecosystem'.

Hadikusuma, R.S., Lukas, L. and Rizaludin, E.M. (2023) 'Methods of stealing personal data on android using a remote administration tool with social engineering techniques', *Ultimatics: Jurnal Teknik Informatika*, 15(1), pp. 44–49.

Haislip, J., Lim, J.-H. and Pinsker, R. (2021) 'The impact of executives' IT expertise on reported data security breaches', *Information Systems Research*, 32(2), pp. 318–334.

Hantrais, L. and Lenihan, A.T. (2021) 'Social dimensions of evidence-based policy in a digital society', *Contemporary Social Science*, 16(2), pp. 141–155.

Hawa Apandi, S., Sallim, J. and Mohd Sidek, R. (2020) 'Types of anti-phishing solutions for phishing attack', *IOP Conference Series: Materials Science and Engineering*, 769(1), p. 012072. Available at: https://doi.org/10.1088/1757-899X/769/1/012072.

Heartfield, R. and Loukas, G. (2015a) 'A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks', *ACM Computing Surveys (CSUR)*, 48(3), pp. 1–39.

Heartfield, R. and Loukas, G. (2015b) 'A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks', *ACM Computing Surveys (CSUR)*, 48(3), pp. 1–39.

Hijji, M. and Alam, G. (2021) 'A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions', *Ieee Access*, 9, pp. 7152–7169.

Hove, L.T. (2020) 'Strategies Used to Mitigate Social Engineering Attacks'.

Huang, Y. *et al.* (2019) 'An adversarial learning approach for machine prognostic health management', in *2019 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS)*. IEEE, pp. 163–168.

Huseynov, F. and Ozdenizci Kose, B. (2022) 'Using Machine Learning Algorithms to Predict Individuals' Tendency to be Victim of Social Engineering Attacks', *Information Development*, pp. 1–21. Available at: https://doi.org/10.1177/02666669221116336.

Huseynov, F. and Ozdenizci Kose, B. (2024) 'Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks', *Information Development*, 40(2), pp. 298–318.

Hussain, M., Siddiqui, S. and Islam, N. (2023) 'Social Engineering and Data Privacy', in *Fraud Prevention, Confidentiality, and Data Security for Modern Businesses*. IGI Global, pp. 225–248.

IEEE Xplore Full-Text PDF: (no date a). Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9312039 (Accessed: 20 February 2024).

IEEE Xplore Full-Text PDF: (no date b). Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9087851 (Accessed: 20 February 2024).

IEEE Xplore Full-Text PDF: (no date c). Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9323026 (Accessed: 20 February 2024).

Illi, E. *et al.* (2023) 'Physical layer security for authentication, confidentiality, and malicious node detection: a paradigm shift in securing IoT networks', *IEEE Communications Surveys & Tutorials*, 26(1), pp. 347–388.

Jain, A.K. and Gupta, B.B. (2022) 'A survey of phishing attack techniques, defence mechanisms and open research challenges', *Enterprise Information Systems*, 16(4), pp. 527–565. Available at: https://doi.org/10.1080/17517575.2021.1896786.

Keserwani, H. *et al.* (2022) 'Security Enhancement by Identifying Attacks Using Machine Learning for 5G Network', *International Journal of Communication Networks and Information Security (IJCNIS)*, 14, pp. 124–141. Available at: https://doi.org/10.17762/ijcnis.v14i2.5494.

Korkmaz, M., Sahingoz, O. and Diri, B. (2020) *Detection of Phishing Websites by Using Machine Learning-Based URL Analysis*, p. 7. Available at: https://doi.org/10.1109/ICCCNT49239.2020.9225561.

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

Krombholz, K. *et al*. (2015) 'Advanced social engineering attacks', *Journal of Information Security and Applications*, 22, pp. 113–122. Available at: https://doi.org/10.1016/j.jisa.20