IJECBE

IJECBE (2025), **3**, **1**, 188–211
Received (26 November 2024) / Revised (23 December 2024)
Accepted (26 December 2024) / Published (30 May 2025)
https://doi.org/10.62146/ijecbe.v3i1.103
https://ijecbe.ui.ac.id
ISSN 3026-5258

International Journal of Electrical, Computer and Biomedical Engineering

RESEARCH ARTICLE

RTBTS: A Real-Time Behavioural Training System to Mitigate Psychological Vulnerabilities in Social Engineering Attacks

Narendar Kumar* and Muhammad Salman

Department of Electrical Engineering, Unversitas Indonesia, Depok, Indonesia
*Corresponding author. Email: narendarkumaroad@gmail.com

Abstract

The aim of this research is to identify the psychological traits that make people susceptible to social engineering attacks and the effectiveness of current cybersecurity training. The study tries to identify how these factors can be better utilized to enhance the resilience of individuals in response to such an attack, due to a psychological or training deficiency. This involves data collection through structured surveying on internet platforms such as Google Forms. The analysis has been done by means of Python using statistical techniques, focusing on the descriptive analysis and regression analyses that set the links of psychological features and sensitivity to social engineering influenced by training programs. It followed from the research that certain psychological features of a person, like a high level of trust without its verification and readiness to conform with authority, raise his or her susceptibility to social engineering essentially. The training programs assessment had shown positive attitude to their helpfulness though deficiencies in adaptability and frequency of trainings reduce its potential to neutralize sophisticated social engineering techniques. These results reflect that, although the existing training is fairly successful, there is an urgent need for more flexible training methods that would consider individual psychological profiles and be updated regularly in combat with emerging social engineering strategies. Guided by these considerations above, this research supports the establishment of a Real-Time Behavioural Training System, RTBTS, continuous monitoring of dangers for dynamic adapted training modules.

Keywords: Social Engineering, Psychological Vulnerability, Cybersecurity Training, Real-Time Behavioural Training System (RTBTS), Adaptive Learning, Behavioural Monitoring, Threat Analysis

1. Introduction

1.1 Background

In today's fast growing and technologically evolving era world is promptly transforming with the advent of revolutionary technologies such as 5G+ and artificial intelligence, machine learning and other data driven technologies. With this immense dependence on technology at first hand where it has many benefits on the other hand poses a serious cyber threat that can and as proved in past has potential to disrupt the services and network of this interconnected world with serious consequences.

Though, considering the occurrence of cyberattacks in this digital world there are a lot of digital defences available to curb that threat considering various types of cyberattacks. However, social Engineering is such a technique that has potential to bypass all the technologies and modern digital defences[1]. social engineering is a technique or a type of attack where in an adversary exploits human psychology to gain access to the systems[2]. That's why cybersecurity experts commonly view the user as the weakest link in this chain, which gets limited attention. This limited attention and awareness can create vulnerabilities such as fear, urgency, curiosity and authority to which malicious actors may take advantage. Given the relative comparison between technical vulnerabilities and human errors, it is justifiable to call humans the weakest link in the computer security chain[3]. For example, despite the invention of authentication technologies such as fingerprint identification, voice recognition, or retinal scanning, the careless or intentional misuse of passwords could easily compromise a technically sound authentication system that has been built and used for years.

That is according to Worldmetrics.org, In 2024, phishing which is a type of social engineering attack accounted for approximately 98 percent of all cyberattacks. However, as visualized in figure 02, according to Bolster research report, AI-powered social engineering tricks and phishing attacks have also increased because, according to the research report more than 38 000 phishing sites come into being in just one day in the first half of 2024[4]. More attackers take a multichannel approach in using email, text messaging, social media, fake websites, and voice calls-greatly expanding their attack surface in these aspects. Phishing attacks linked to social media increased 170%. And while 75 percent of all nation-state actorsthat is, primarily China, Russia, and Iran-are responsible for these phishing attacks and data breaches involving matters pertaining to the president. In May, there were phishing attacks doubled, compared to the same time last year, against summer consumers. Most of the attacks fell onto the technology sector, accounting for 67% of all phishing attempts, while payment providers, because of their high value in resale and high profitability, received 15% more of these attacks[4].

Social engineering approaches have been a great contributor to unauthorized network breaches in the year 2023, at times referred to as "hacking humans." In this year, there was a strong uptick across these attacks noticeably in the third quarter. One of the first access methods, phishing rose 8% to be the most frequent strategy in Q3 with a 46% share. There was also a 9% increase in leveraging genuine accounts to 21%, while methods related to social engineering, such as voice phishing-also known as vishing-and others increased 3%. Overall, the increase represents an alarming spike in the use of human-targeted attack vectors[5].

At 29%, phishing remained one of the most serious attack vectors of 2022, while most serious cyberattacks could have been prevented if users were better trained to recognize and react appropriately to phishing emails. Perhaps the most common such tactics included phishing with pages made to look like Microsoft 365 using session cookies to bypass multi-factor verification. Attackers used spoofed UN organization names in order to dupe victims into disclosing passwords or personally identifiable information. Some of such schemes had such domains in the threads of the emails, which were targeting espionage. During Q3, social engineering attacks did not let up, as more than 1,300,000 phishing sites were identified, up 15% from Q2 of 2022[6].

Also, 255 million malicious URLs were spotted, which was up by 61% from the figure recorded in 2021. Further, 79% of the firms were found to be attacked by spear phishing, while mobile phishing attacks increased by 50%. Despite security and awareness drives, breaches due to phishing have crossed the $52 million mark in terms of financial losses. It has, in 2021 alone, witnessed a 29% increase in the incidence of phishing, while retail and wholesale sectors attacks increased by 436%, with impersonation making up to 49% of the threats. The instances of SMS phishing have seen a jump of 700%, while breach costs have been touted at an average of $4.91 million-meaning there is an urgent need for more extensive security measures[7].

1.2 Problem Statement

Though various cognitive and psychological taxonomies have been proposed in the literature to provide an effective defends against the social engineering cyberattack, underlining both human and technical components contributing to these threats. These will form the basis for devising a comprehensive defence measure that reduces the vulnerabilities taken advantage of by adversaries yet need to be improved considering the latest techniques, tactics and procedures of the adversaries and taking into account the real-world case studies. Besides, several other factors have been excluded that still making a social engineering a real problem such as challenges in detection accuracy and lack of standardized protective measures, many studies overlook target context and cognitive processes, Limited empirical evaluation of AI countermeasure, lacks empirical testing of prevention and mitigation strategies; limited analysis on socio technical and psychological impacts, limited regional and sample size collection and not addressing human factors are one of the main contributors to the social engineering tally. Aforementioned shortcoming in the proposed defences against the emerging social engineering attacks requires a more comprehensive attention in order to formulate a more effective technical and cognitive defence strategy

1.3 Aims and Scope of the Research

The aim of this study is to find out what psychological factors make such social engineering attacks successful and to outline certain rules of behaviour that could reduce such risks. This research will now examine exactly which psychological triggers, such as trust, fear, urgency, and authority, social engineers use in trying to dupe people into revealing confidential information or into taking an action that would result in a breach of security. The research will focus on the enhancement of protection mechanisms design based on the apprehension of basic psychological factors that emphasize improvement in awareness, cognitive defence hardening, and training programs targeting these vulnerabilities.

This research focuses on the attackers who use social engineering strategies, the potential victim endusers, and cybersecurity experts and organizations tasked with providing security training programs. It outlines both existing and new methods of social engineering in collaboration with historical techniques to give a total outlook on past and present trends. This research applies to corporate environments, public sectors, and individuals in different geographical and industrial contexts. This research aims to address the growing risk of social engineering, an attack vector that uses psychological manipulation to bypass security, by enhancing current defense mechanisms and strengthening user-level defenses. This will be reached by conducting a deep study of attacker methodologies, comprehensive surveys of established and emergent techniques, reviews of current protective measures such as training and awareness programs, and recommendations for improvement founded on principles of psychological resilience. The data collection will involve surveys, case studies, and literature review that will ensure practical insight and an overall strategy in handling issues related to social engineering.

2. Literature Review

2.1 Social Engineering Concepts and Attack Lifecycle

In the realm of cybersecurity, the concept of social engineering refers to a particular type of attack that is carried out by exploiting the human psychology being the weakest component in the chain of cybersecurity world. Social engineering is often termed as a “Human Hack” because an adversary takes the advantages of human weaknesses such as fear, authority, curiosity, urgency, trust and greediness to manipulate an individual to access sensitive information to perform further actions[8]. In general, the methodology of social engineering attacks includes four major steps: information gathering, relationship building, exploitation, and execution[9]. Because most attacks depend on the effectiveness of the information-gathering step, attackers tend to spend most of their time and resources on the first stage. Most attacks begin by taking advantage of the sheer volume of public information available freely from people posting details about their personal lives online, especially on social networking sites. This information could be used either directly in the attack or to obtain further information from secondary sources. Given below in figure 01 is the flowchart that represents the social engineering attack lifecycle and along with various stages followed by a typical adversary to carryout social engineering attacks also explained below

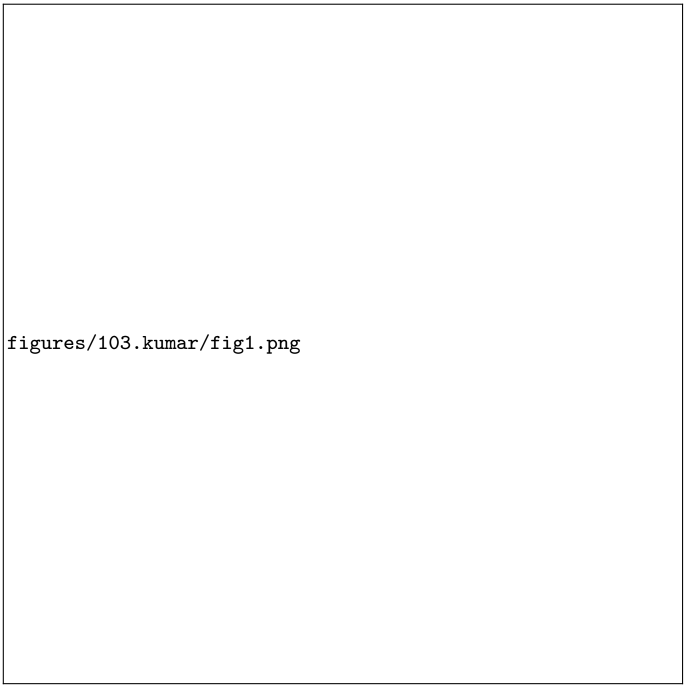

Figure 1. Represents a complete lifecycle of a typical social engineering attack

i. *Target Identification*

This first step involves an attack against either an individual or organization that might be targeted with regard to vulnerabilities, roles, or access to important information. They may also target highvalue targets such as executives, finance personnel, or IT administrators. This stage is important because it helps attackers filter their targets toward those most likely to provide the needed information or give access.

ii. *Information Gathering*

These social engineering attacks primarily rely on the first step of information gathering, during which the attackers will make use of open-sourced data, particularly from social networks. This step is fundamental since it provides a foundation for the other steps, such as relationship establishment, exploitation, and execution. In order to trick people into giving away key information, the attackers make use of many deceitful techniques; hence, this step is the focal point of their whole plan[10].

iii. *Relationship Building*

Relationship building by attackers is the process of initiating contact with the target, often under the guise of a trusted individual or organization, while applying manipulative psychological strategies in order to build trust. This manipulation reduces the target's defenses, making them even more vulnerable to the succeeding exploitation. In order to set the stage for potential exploitation, attackers employ a number of ways to generate trust and minimize suspicion[11].

iv. *Exploitation*

The exploitation step in cyberattacks is about influencing targets to conduct activities that benefit the attacker, many times using psychological cues such as urgency, authority, or curiosity. This step in the process is really quite critical in that it bridges established trust into actionable outcomes for the attacker. In fact, much of the psychological and cognitive aspects involved with this process lead to both the target's vulnerabilities and the techniques adopted by the attackers. Poor management of one's emotions and a higher degree of persuadable can be named among the psychological variables that increase the vulnerability to victimization. Poor socioeconomic state and cognitive decline are also particularly vulnerable because they will not even be able to recognize what is being perpetrated against them and take countermeasures[12].

v. *Execution*

Finally, after compromising a target, social engineering attacks usually try to achieve goals such as data theft, financial fraud[10][13], malware installation, or unauthorized access to restricted locations[14]. Indeed, such attacks usually lead to data theft when an attacker uses the information acquired to access sensitive data, which results in identity theft and financial fraud, or may also be utilized in gaining physical entry to restricted areas within an organization. These kits exploit software vulnerabilities in social engineering attacks for installing malware on target systems, serving harmful payloads to end-users[14].

vi. *Disengagement*

This disengagement phase is very crucial in social engineering to get away from detection and ensure the integrity of their unlawful action. This phase comprises disconnecting the connectivity with the target, removal of digital footprint, and making sure that all proof of the engagement is gone. The whole idea is to keep the attack unseen for as long as possible to give a chance for the attacker to utilize the information gathered without raising unnecessary suspicion. This is an elaboration of social engineering that relies mostly on the psychological manipulation of a target rather than actually hacking into a system through technique. Strategies involve cleaning up or removing digital fingerprints: for example, emails, messages, and other forms of digital communication are often deleted by hackers where they can be traced to the attacker. This helps them not to leave any traceable evidence that can be linked back to them[10][15] and ceasing the communication once the attacker gets possession of the information in need, straightaway, all modes of communications with the target are stopped to keep it from raising suspicion[16].

2.2 Social Engineering Attack Types

Following are some most common and typical types of social engineering attacks.

2.2.1 Phishing

Phishing attacks are the most widespread type of cybercrime in which social engineering methods are utilized to deceive victims with the aim of divulging sensitive information. With their development, the attacks have taken on various forms of communication, including e-mails, websites, and instant messaging. The five basic types of phishing include General Phishing, Spear Phishing, Smishing, Vishing, and

Whaling. All these types of phishing differ in the method that an attack carries out in order to achieve an adverse purpose that generates great harm both to persons and businesses. The following sections elaborate on the features and detection mechanisms of these phishing attacks[17]. According to Bolsters 2024 Mid-Year Phishing Report, an upsurge in phishing attacks, as more than 38,000 New phishing sites come up every day, topping 1.4 million in May. Phishing has moved out of email and on to social media, SMS, and doctored domains, making these attack vectors even more difficult to detect. Social media phishing grew by 170%, while technology at 67% took the pole position because of the data's high value. The financial sectors and e-commerce were also heavily targeted. A total of about 3.4 million phishing domains called the U.S. their home, accounting for approximately two-thirds of all phishing sites, and showing just how economically and digitally appealing it was. It underscores a growing need for an effective multi-channel cybersecurity defence that can push back mounting sophistication and volume in such attacks. In the figure 01, it can be observed that technology sector is the most affected sector by phishing until the mid of year 2024 with 67%.

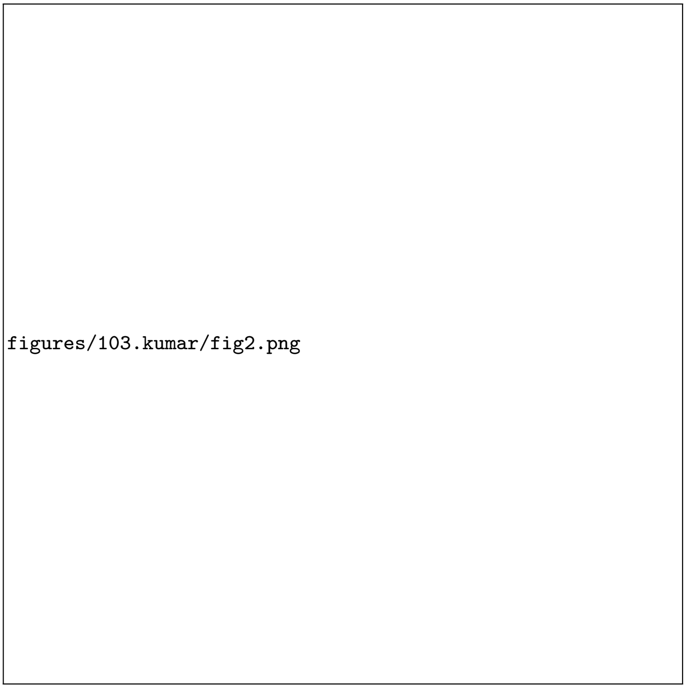

Figure 2. Shows pie chart representing overall sectors affected by phishing attacks (Bolsters Mid-2024 report)

2.2.2 Baiting

Baiting is a form of social engineering attack that manipulates individuals through the promise of a desirable object-for instance, free software or movies-to influence

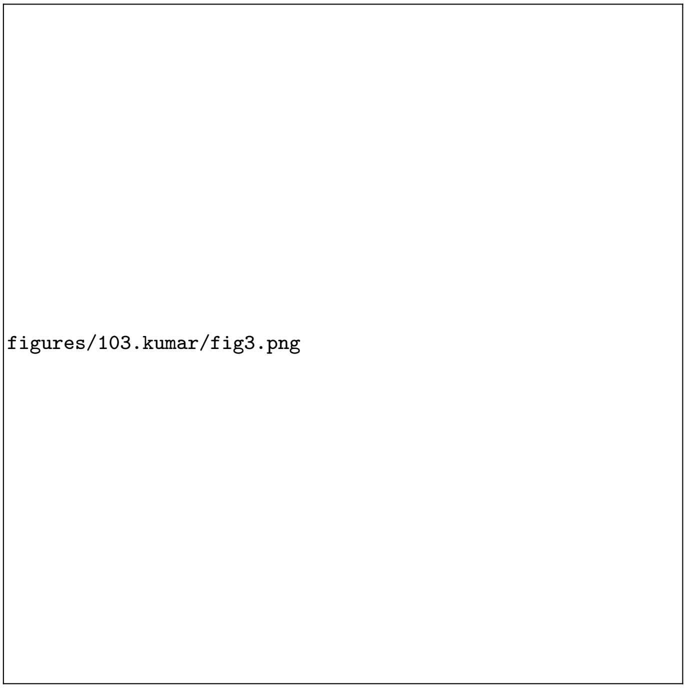

Figure 3. Shows average phishing attacks globally, per month in the first six months of the year 2024 (https://bolster.ai/2024-mid-year-phishing-report).

and affect their activities. This often involves the use of malware-carrying devices, such as flash drives, left at strategic locations to attract others into compromising their systems by accessing the device[18]. Honeypots are another form of software bait but are utilized essentially for detection, deflection, or research of hacking attempts by emulating vulnerable systems[18]. They do differ in complexity and serve practical purposes as well as scientific objectives when it comes to understanding cyber dangers.

2.2.3 QUID PRO QUO

The Latin phrase "quid pro quo" means "something for something" or "this for that". A quid pro quo attack is a form of social engineering where the attacker offers some sort of service or a gift in return for the sensitive information or access. For instance, an attacker can masquerade as an IT support expert and offer aid to a victim who might be experiencing technical problems whose solution involves the victim releasing sensitive information-such as his or her login credentials[19].

2.2.4 Water Hole

Watering hole attack in social engineering gets its name from a realistic scenario in which the predator would linger around the waterholes, awaiting their target prey to finally come and drink. Similarly, in this approach, the attacker chooses a website that the target often opens and then compromises it by infecting the site with malware.

When the intended target opens the contaminated site, he unknowingly downloads malicious code, giving the hacker access to his system[20].

2.2.5 Dumpster Diving

Dumpster diving is a social engineering approach in which the criminal rummages through trash in search of valuable information. This method is very often overlooked, since most people do not understand the risks involved with the improper disposal of sensitive documents and technology. Failure to utilize proper disposal methods, such as shredding documents and securely wiping digital files, allows malicious individuals to collect materials with which to strike. Such behaviour demands greater awareness and countermeasures[21].

2.2.6 Pretexting

Pretexting is one social engineering method where the attackers create a scenario and then pretend to be a high-level individual or a very trusted source, like fellow employees, police, or even bank employees, to build trust with the victim to ask them for something valuable in the form of information or for certain actions. Since it manipulates the victims through a feeling of legitimacy of a situation, it's considered one of the widely used threats in social engineering attacks against social networks[10].

2.2.7 Shoulder Surfing

Shoulder surfing is a direct observation attack intended to view the screen or keyboard over another person's shoulder to access personal information. In such a case, it has mostly been used to retrieve authentication information, such as PINs and passwords, along with other confidential information for malicious reasons. In this respect, research shows that attacks through shoulder surfing pose great a danger to sensitive information, which calls for the development of secure authentication methods that may withstand vulnerabilities at the cost of usability versus security[22].

2.2.8 Tailgating

Tailgating, or "piggybacking," is a social engineering attack in which an unauthorized individual closely tags behind a person who does have legitimate access to a restricted area. The attackers may use several methods to tailgate, including but not limited to: disguising themselves as deliverymen, acting confused, or asking for help in holding the door open. This method depends on proximity to successfully get around security mechanisms, which would include access control systems, checks to identify the person, and on-duty security guards, serving to remind us how important awareness is to maintain set standards of security within sensitive areas[23].

2.2.9 Scareware

Scareware is a form of cyberattack that incorporates social engineering in order to make consumers feel like their devices have been infected, thus pushing them into downloading sham security programs. An attack of this nature employs anxiety and a lack of technical awareness amongst consumers by creating pop-ups similar in nature to actual security warnings. This is how people might get tricked into installing malicious software to cause further malware infections or data theft and financial loss. The ensuing sections outline the mechanism and implications of scareware assaults, using appropriate inputs from the research publications provided[24][25].

2.2.10 Reverse Social Engineering

In such an attack, the attacker creates a situation in which the victim feels obliged to call him to seek help or information. In such an attack, for instance, the attacker may initiate some kind of technical problem and then masquerade as an expert capable of trying it. Afterwards, the victim may reveal confidential information to the attacker, believing this to be an exchange with authoritative authorities[24].

2.3 Psychological Factors in Social Engineering

Social engineering attacks usually encompass numerous psychological principles in trying to get individuals to divulge information or execute an act that, otherwise, would not be considered. One of the major frameworks in ascertaining the said psychological dynamics is that propounded by Robert Cialdini known as the principles of persuasion. The principle of reciprocity installs indebtedness; hence, the victim returns the Favor[10]. Commitment and consistency take advantage of the desire of people to be consistent with their previous actions, social proof entices by pressures others' behaviour while building trust, authority plays on impersonation with figures in power to make people comply, liking utilizes friendliness to manipulate targets through rapport, and scarcity is urgency to make them act in haste[26].

By combining all these factors, attackers successfully create scenarios to leverage the human tendencies of trust, conformance, and urgent decision-making-the awareness and education relationship to such an attack serve to try to prevent it or deter it. In social engineering, these concepts are applied to manipulate human propensity or trust, obedience, and appealing to social proof. Of particular importance are individual differences, such as personality traits, in the vulnerability of targets to social engineering attacks. Among the traits that elevate one's level of gullibility, high agreeableness, openness, low conscientiousness, and high neuroticism stand out. These psychological factors, once identified, should set a basis for developing effective countermeasures and training programs against social engineering threats. Agreeable individuals easily give their trust to people and readily give in to requests. Thus, highly agreeable individuals are potential victims of social engineering attacks such as phishing and impersonation[27][28]. High openness is described as curiosity and the tendency to be open to trying new experiences[29]. This perhaps may motivate users to interact with unknown links or data, and they tend to easily fall for baiting techniques[30]. Individuals with low conscientiousness are characterized by lack of attention to detail and careful work, hence leading to vulnerability to being misled into scam schemes, for instance, phishing attempts. In addition, the individuals with high neuroticism show higher level of stress and anxiety; thus, may get readily vulnerable to urgent or fear-relevant cues which results in making quick judgments without adequately weighing risks[31].

A weaker tendency for risk awareness could make individuals more vulnerable in cases of social engineering attacks, given that one cannot detect or appropriately assess the potential threats[28]. Inability to develop self-efficacy, or belief in one's abilities to deal with security challenges, also increases vulnerability because people feel less able to resist the manipulation process[30].

2.4 Mitigating Strategies

2.4.1 Non-Technical Preventive Measures

The human element in cybersecurity is a huge weakness; hence, non-technical measures become highly essential for the neutralization of social engineering threats. In social engineering, exploitation of human trust and mistakes are manipulated to achieve objectives, which often evade technical controls. Thus, an effective security plan will comprise full-scale technical and non-technical measures. The urgent need is employee training and education to make employees aware and resilient in case of any social engineering attempt, while audits and compliance measures ensure the adherence to standards of security[27], [28]. With multi-tiered mechanisms, these techniques have come together to fortify organizations against social engineering attacks. Given below are some non-technical prevention measures.

- *Employees Training and Awareness:* Social engineering attacks exploit the vulnerabilities in human nature, and as such, it requires regular training on user awareness. Such training allows the employees to spot the threats and act appropriately, for instance, phishing, vishing, impersonation, among others. All staff should be given regular training that should involve inductions and monthly refresher sessions for high levels of awareness and preparedness[29].
- *Security Policies and Audits:* The security policy should include technical and non-technical measures that can put the security practices in correspondence with the business objectives[32]. Auditing acts as detective controls to identify policy violations and abnormalities which may point to breaches. Audits include periodic reviews of network activities log and user rights[28].
- *Multi-layered Defense Mechanisms*: The latter consideration mentioned above includes the "Defense in Depth" strategy that comprises more technical protections, like two-factor authentication and physical token-based access[28]. The model of defense-in-depth ensures that even when one layer is breached, others will be defending an organization[32].

2.4.2 Physical Guidance

Physical assets can be protected through several methods. Security guards, mantraps, and security cameras can be used in a combined way to deter intruders from entering the premises. In cases where actual hardware is installed, organizations should use multi-factor authentication, biometrics, or an access control list before allowing access.

2.4.3 Technical Prevention Measures

Since social engineering attacks involve both human-centric and technical aspects, a holistic approach in combating them needs to involve these very two spheres. Social engineering is performed by bypassing technical defenses through human psychology; therefore, technological as well as human vulnerabilities must be addressed. Most of the time, technical measures can potentially reduce the chances of such attacks by at least a huge margin through appropriate installation of security protocols and systems. The protection of data and critical infrastructure should be enabled through a multi-tiered defense plan that incorporates both non-technical and technological security controls. MFA makes access control even more restrictive because several verifying factors will be needed to grant access, reducing the risk of unauthorized access by stolen credentials[33]. Regular updating and patching reduce the known vulnerabilities, while segmentation of the network limits the attack surface by sectioning off parts of the network. Intrusion Detection and Prevention Systems monitor and take action against suspicious activities, while firewalls also do the same-a proactive security against potential breaches. All the external-facing services shall be placed behind a DMZ to add protection for the data in transit, such as web filters and VPNs. Data encryption ensures that even if intercepted, sensitive information remains unreadable, both at rest and in transit[19].

3. Research Methodology

3.1 Research Design

This Mix methods research study investigated the psychological factors predisposing individuals to vulnerability in social engineering and the effectiveness of training and awareness programs in minimizing such vulnerabilities. Particularly, explanatory sequential mixed-methods study encompassed the quantitative data collection and analysis stage before the integration of qualitative data findings from literature and quoted case studies. This survey data learnt the interpretation and contextualizing of findings supported by published work on psychological variables in social engineering.

This study design allowed a demanding understanding of the links amongst psychological traits and vulnerability, supported by theoretical input in order to establish and build on the findings. The research was designed around a survey that examined a number of psychological features, responses to social engineering scenarios, and the apparent efficiency of existing cybersecurity training, including the defence mechanism against aforementioned vulnerabilities.

The research had two systematic stages. It first gathered quantitative data by using the systematic questionnaire under Google Forms, gathering demographic data, psychological measures, awareness, and history of the participants in trainings. Phase two involved the inclusion of the qualitative data, including analysis of the open-ended survey data and data gathered under the use of scholarly literature and cyber security breach case studies. This supported the interpretation of statistical trends more intensively, particularly on the effectiveness of the trainings and the measures of psychological resilience. Quantitative findings supported the thematic interpretation, situating the study in the explanatory sequential mixed method design.

3.2 Research Questions

- Which psychological characteristics, such as trust, fear, and authority, are frequently manipulated in social engineering attacks?

- What is the impact of various demographic parameters, such as age, education, and professional history, on an individual's vulnerability to social engineering?
- How effective are existing training and awareness programs in minimizing the risks of social engineering? What modifications may be made to enhance the effectiveness of these programs?

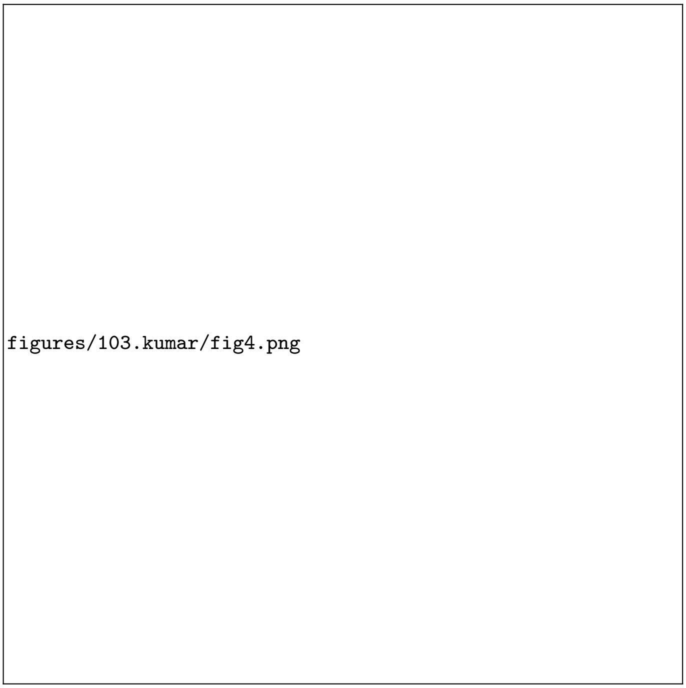

Figure 4. Overview of the research methodology

3.3 Data Collection

Data collection was done electronically through Google Forms, allowing not only efficient distribution but also effortless response collection across different regions. The survey had a total of 200 participants, recruited via internet-based channels. The questionnaire consisted of 20 questions, addressed under the topics of demographics, psychological characteristics, social engineering awareness, cyber security training, and improvement areas. Most items were on a five-point Likert scale from "Strongly Disagree" (1) to "Strongly Agree" (5), and two questions (Q18 and Q19) had the provisions of open-ended qualitative answers in order to obtain the participants' contribution of suggestions. No interviews or focus group discussions were held; however, qualitative analysis was conducted using these two questions along with findings drawn from scholarly papers and case studies in order to contextually support the quantitative results. The questionnaire ensured anonymity and confidentiality to garner honest and accurate responses.

3.3.1 Validity and Reliability

To ensure content validity, the questionnaire was developed through a literature synthesis and validated by expert academic peer review in both the fields of behavioral science and cybersecurity. While pilot testing and statistical measures of reliability (i.e., Cronbach's alpha) were not conducted, the items on the questionnaire were measuring established social engineering research constructs. Future methodological soundness of research could be improved by pilot testing and using psychometric testing of reliability to establish the validity of the instrument more conclusively. Since interviews were not a part of this study, procedures in regard to inter-rater reliability were not necessary.

3.4 Data Analysis

Acquired data was analyzed using Python for statistical computing to make sure the data was correct and efficient. Descriptive statistics were produced to describe the data and identify distribution and key patterns of answers. The correlation analysis was performed to study the links between distinct psychological qualities and their impact on vulnerability to social engineering, while regression analysis was also applied to investigate the impact of training programs with an emphasis on changes in awareness and behavior before and after training interventions.

4. Results

4.1 Demographic Profile of Respondents

This chapter provides a demographic profile of the data of the 200 survey participants who contributed to the study. It includes data on their gender, age, education, occupation, and work experience in years. The majority of the respondents (48.3%) were in the 21–30 bracket, followed by 26.9% in the 31–40 bracket, with smaller numbers in the 18–20 (13.9%), the 41–50 (10.4%), and under 18 (0.5%) brackets. By gender, the majority (60.2%) identified themselves as male, and females made up 39.3% of the sample, with minimal duplication of the entry of "male" (0.5%). By education, the sample was well-qualified: 41.8% had postgraduate qualifications, 40.8% had undergraduate qualifications, and the remainder had high school (10%) or doctorate (7%) qualifications. Professionally, the respondents had a mixed background: non-IT students (31.3%), IT professionals (26.4%), non-IT professionals (25.4%), and IT students (16.4%), and minimal duplication of entries (0.5%).

In work experience, the largest proportion was one year of experience (43.8%), then 1–5 years of experience (27.9%), 6–10 years of experience (15.4%), and above 10 years of experience (12.4%). This distribution in the sample provides transparent contextual rationale for the examination of social engineering perceptions' psychological and behaviour tendencies and the applicability of social engineering instruction. The demographics provide context in which different user populations perceive and respond to social engineering threats

4.1.1 Perceived Effectiveness of Training Programs

The average ranking for the perceived efficacy of cybersecurity training is 3.89, indicating overall agreement among subjects that such training has value in reducing their risk. Above a moderate rating, this supports the generally favourable impression of the influence of cybersecurity training. The median, 4, is not far behind and indicates that the typical respondent agrees that frequent training greatly lessens the danger associated with social engineering attacks. However, the range of ratings extends to a minimum of 1, showing that a minority of participants are suspicious about the efficacy of the training. The first quartile is at 3, indicating that a quarter of the replies rank the performance of the training as no more than fair, showing a degree of skepticism or perceived limitations in these programs. Contrarily, the third quartile reaches 5, showing that a high 75% of the respondents rate the effectiveness as moderate to very high.

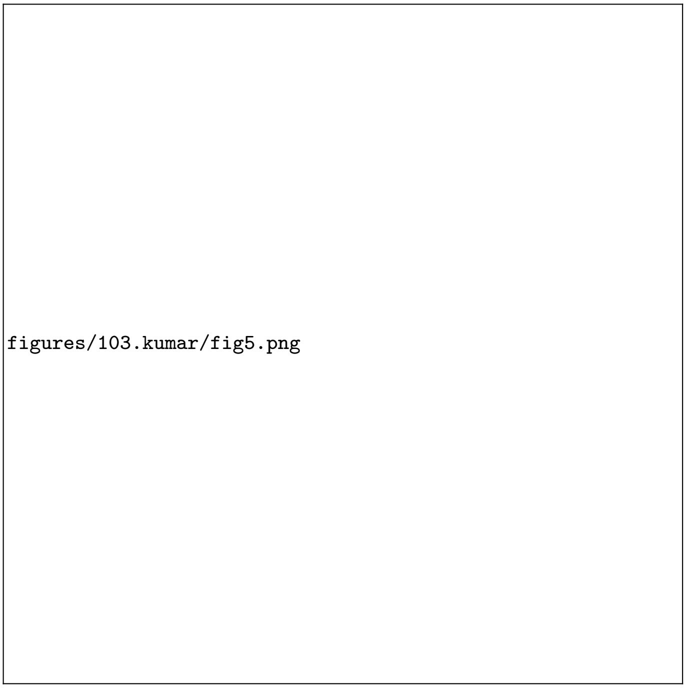

Figure 5. Represents the efficacy of cybersecurity, in particular social engineering awareness training over several metrics

4.1.2 Perception of trust and Authority

In the research on trust without verification, the participants were to rate their likelihood of trusting others without verification; the mean score was 2.395, which suggested a moderate level of suspicion. Where the median is a little below the midpoint at 2.0, together with a minimum score of 1, that would indicate that a large fraction of participants are very unlikely to extend trust without verification, with at least 25% showing a strong level of distrust as the lower quartile stands at 1, whereas on the opposite side, the top quartile is 3, showing that up to 75% of the respondents keep their trust level at or below moderate as shown below in the table 01.

Table 1. Perception of trust and Authority values

Metric	Trust Without Verification	Compliance With Authority
Mean	2.395	3.945
Median	2.0	4.0
Minimum	1.0	1.0
Lower Quartile	1.0	3.0
Upper Quartile	3.0	5.0

In fact, the figures would suggest a somewhat greater tendency toward obedience to authority-3.945 average score-when testing for conformity to authority. The median score is 4, supporting this result to indicate a general predisposition of people to comply, with the majority complying or strongly complying as the upper quartile is at 5. On the other hand, a minimum score of 1 and a lower quartile at 3 hints at some resistance among a few, indicating varied degrees of conformity within the group.

4.1.3 Correlation between Trust, Authority and Compliance

A reasonably strong positive correlation of 0.65 now shows that persons more likely to trust without verification are also apt to comply with requests from authorities. This may indicate a general respect for the authority figure himself and a readiness to receive information or orders without inspection, presumably in accord with the ideas in social cognitive theories concerning the legitimacy implied in trusting authorities, leading ultimately to better compliance.

Another, somewhat weaker, correlation of 0.54 between trust without verification and response to urgent requests indicates that those who easily trust might respond more to urgent situations, especially those dealing with work or finances. This could be considered a behavioural bias in which trust predisposes people to react hastily under pressure, an important consideration in the defenses against social engineering. Strongest of all observed correlations was 0.70 with compliance and response to urgent requests; this suggests that a very sizeable positive correlation exits, implying that individuals compliant with authority are more likely to respond readily to urgent demands, which can be thought of in terms of obedience to authority, adding an extra layer of pressure that heightens compliance.

Table 2. Shows correlations between Trust, Authority and Compliance

Correlation Pair	Correlation Coefficient	Strength & Interpretation	Theoretical Implication
Trust Without Verification & Compliance with Authority	0.65	This is a reasonably substantial and positive correlation, demonstrating that persons who are more prone to trust others without verifying their identities also tend to comply with requests from those in positions of power. This could reflect a general predisposition towards deference or confidence in authoritative figures.	This relationship could be based in social cognitive theories which posit that trust in authority can lead to higher compliance due to perceived validity or expertise.
Trust Without Verification & Response to Urgent Requests	0.54	This correlation is positive but marginally weaker than the first. It signifies that individuals who trust easily are also somewhat more likely to respond to urgent requests, especially those related to work or financial matters.	This may show a behavioural bias where trust inclines individuals to react more hurriedly under pressure, potentially bypassing normal verification processes due to an urgency bias.
Compliance with Authority & Response to Urgent Requests	0.70	Strongest correlation observed, demonstrating a significant positive relationship. It suggests that those who generally comply with authority also incline to respond more eagerly to urgent requests.	The high correlation can be understood through the lens of obedience to authority, where urgency adds an additional layer of pressure that may further increase compliance.

These correlations reflect a consistent behavioural pattern in which trust and obedience to authority go hand in hand with enhanced responsiveness in emergent situations, with important implications of psychological traits as modulators of human behaviour in the structured environment of workplaces or emergency management. It is also useful during the discussion of the research paper, linking with the existing literature on trust, authority, and behavioural responses, while contributing a great deal to psychological and organizational studies through its inquiry into the way intrinsic traits affect decision and compliance in many scenarios.

4.2 Regression Analysis

This regression analysis was supposed to examine the factors affecting individuals' perceived vulnerability to social engineering attempts. For this purpose, it used a sample dataset of 200 observations. In this, it has regressed a dependent variable of the people's self-assessed vulnerability rated on a scale from 1 to 5, on the following predictors: trust in people without checking their identity, obedience to authority, promptitude of response to urgent requests, following orders when under pressure, awareness of social engineering attacks, and awareness of tactics used in social engineering attacks.

Table 3. Shows the model summary

Dependant Variable: Vulnerability		**R-squared:**		0.079		
Independent Variables	**coef**	**std err**	**t**	$P > \|t\|$	**[0.025**	**0.975]**
Trust people without verifying their identity	0.3300	0.092	3.576	0.000	0.148	0.512
Compliance with a request when made by someone in authority (e.g., a supervisor or official)	-0.1270	0.111	-1.140	0.256	-0.347	0.093
Responding to urgent requests, especially when related to work or financial matters	-0.1137	0.113	-1.007	0.315	-0.336	0.109
Following instructions when you feel pressured or stressed	-0.0118	0.115	-0.103	0.918	-0.238	0.215
Knowledge About Social Engineering Attacks	0.3507	0.255	1.376	0.170	-0.152	0.853
Awareness of The Tactics Used in Social Engineering Attacks (E.G., Phishing, Baiting, Pretexting)	-0.2363	0.226	-1.045	0.298	-0.682	0.210

The regression model carried out in this study gave an R-square of 0.079, indicating that about 7.9% of the variance in the perceived vulnerability of a person to social engineering is explained by the independent variables that have been included in the model. The adjusted R-square was relatively lower, 0.050, which gave a limited explanation of the variability considering the number of predictors applied. This is further supported by the statistical significance of the model with the F-statistic being 2.759 and a p-value of 0.0135, indicating that at conventional significance levels, the chosen variables are significantly associated with felt vulnerability. Of the coefficients tested, trusting persons without verification was significant at a beta coefficient of 0.330 and a p-value less than 0.001, which would indicate that greater trust without verification associated with greater perceived vulnerability, which would make sense because trusting strangers without proof would presumably increase one's vulnerability to social engineering. However, authority compliance was found not to influence vulnerability significantly enough (β = -0.127, p = 0.256), suggesting that conformity by itself is not considered influential on perceived vulnerability.

Responding to urgent requests and instruction when pressed also do not relate with the perception of vulnerability at significant levels, respectively having a probability value of 0.315 and 0.918. Similarly, while the awareness of social engineering attacks showed a positive but non-significant influence on vulnerability, β = 0.351, p = 0.170, it does show a possible trend that with increased awareness, perceived vulnerability may slightly increase, probably because of greater recognition of associated risks. On the other hand, for awareness of specific strategies used in social engineering, a negative coefficient was obtained, β = -0.236, though not significant, indicating basic awareness of tactics is insufficient to reduce perceived susceptibility.

5. Proposed Novel Defense Mechanism: Real-Time Behavioral Training System (Rtbts)

In this regard, the paper proposes a new defense mechanism called the Real-Time Behavioral Training System that would reduce susceptibility through social engineering by addressing individual psychological vulnerabilities with adaptive, situation-specific educational interventions. Components of RTBTS:

- Behavioral Profiling: RTBTS continuously scores individual users on key psychological attributes, such as propensity to trust and obey, through the analysis of Big Data. This is updated regularly to reflect changes in behavior or increased risk exposure.
- Real-Time Monitoring: Integrative with existing cybersecurity frameworks, RTBTS monitors in real time any instance when social engineering risk may occur. This includes unusual request patterns or an unknown source leveraging known vulnerabilities through communications.
- Adaptive Training Modules: RTBTS, if detecting a probable threat situation, will immediately send instantaneous training instructions with context to the user. The adaptive training modules are developed in view of the profile of an individual and the nature of detected danger, building awareness and tactics required for resistance against the kind of social engineering attempt faced.
- Feedback Loop: After interaction, the system requests feedback from users about the effectiveness of the intervention to reassess the behavioral profile and the training modules. The feedback loop guarantees that the system continuously learns new threats and learning improvements of individuals.

5.1 Implementation Considerations:

- Integration into Existing Security Infrastructure: RTBTS has the capacity to be integrated with existing security protocols and systems, thereby complementing and not replacing existing defenses.
- Privacy and Ethical Considerations: RTBTS design will consider privacy and ethical treatment of personal data. In that respect, it should be transparent, and any data collection and profiling should not violate worldwide data protection legislation.

5.2 Expected Impact

The RTBTS has the potential to significantly enhance individual and organizational resistance against social engineering because of its real-time, adaptive training that responds immediately to the immediate threat environment and is personalized to the individual psychological profiles. This way, it will not only train users but also involve them in the process of defense, probably leading to a significant decrease in the number of successful social engineering attacks.

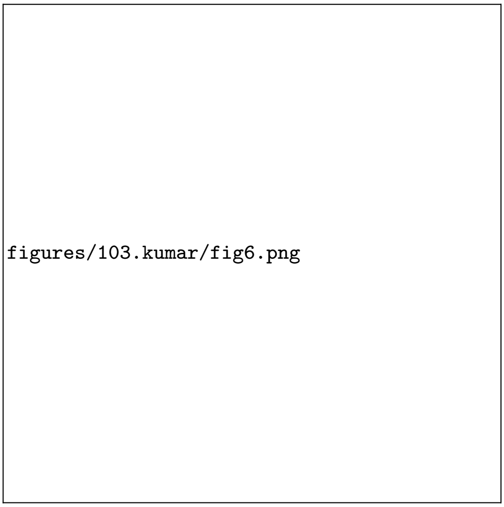

Figure 6. Represents a flowchart for the suggested defense mechanism

6. Discussion

The findings of this study draw on major psychological features through which susceptibility occurs in social engineering, such as trust without any proof and obedience with authority. The outputs of the regression analysis brought into focus an essential role played by these attributes in improving vulnerability of an individual, with trust without verification showing out as a particularly effective predictor. Even though responses are aware of the strategies pertaining to social engineering, awareness alone will not translate into reduced vulnerability-as evidenced by nonsignificant impacts of awareness variables.

Analysis of the training programs generally presents a positive assessment of the effectiveness of the training programs, though a closer look suggests that something is amiss. For example, the frequency and content of existing training may not adequately prepare individuals to counter state-of-the-art social engineering attacks, especially in real-world situations. These findings expose a gap between theoretical effectiveness of training and actual practice, underlining a need for more dynamic and adaptive options.

7. Recommendations

Many of these strategic recommendations have been identified to make cybersecurity training in general more effective, thereby raising overall defenses against social engineering. First, there would be the implementation of Real-Time Behavioral Training Systems (RTBTS). Such adaptive training systems dynamically adapt their training content, reflecting changing individual risk profiles and the changing threat landscape. RTBTS can provide relevant instructional content to the user exactly when they are experiencing potential risks by integrating behavioral profile with real-time monitoring and adaptive responses, which greatly enhances the timeliness and relevance of the interventions.

There is also a dire need to increase the frequency of training. While social engineering methods are in continuous development, training information needs to be updated simultaneously to reflect the current strategies deployed by cybercriminals so that it can retain its relevance and effectiveness. Moreover, training programs should focus on psychological resilience building. Critical thinking, skepticism, and training on noticing and reacting to the social engineering cues will allow for the construction of a stronger barrier against manipulation tricks.

Additionally, customization of the training programs is also highly recommended to meet the varying characteristics of users. Training must be based on job functions, psychological attributes, and behavioral history, and needs to be effective in targeting a specific vulnerability. Second, methods of periodic evaluation need to be put in place continuously in order to check the effectiveness of these training sessions. Integrating feedback loops allows the intentional adaptation of training strategies and content in response to user input and emerging trends, keeping training relevant and responsive to new challenges.

As the Real-Time Behavioral Training System represents part of the key strategic value from a solution developed for the findings of the study, one may want to introduce the RTBTS within the Recommendations section of the published work. This would not only flow from the natural course of the paper-wherein empirical findings go into actionable recommendations-but it would also give emphasis to the RTBTS as an active creation to solve the observed deficiencies of existing training frameworks. This strategic positioning underlines the RTBTS's role as a novel answer to the ongoing problems that social engineering faces and makes sure it will be recognized as an important component in future cybersecurity defense.

8. Conclusion

This research underlines the complexity and pertinence of psychological aspects in susceptibility to social engineering attacks and reviews the effectiveness of current cybersecurity training programs. Confidence without proof and obedience to authority have been found through cautious statistical analysis as two of the major psychological traits which are statistically very significant predictors of a person's vulnerability toward social engineering. These findings underline not only the relevance of psychological awareness in cyber defense but also how human factors can be subtly manipulated by cybercrimes. These generally left a good impression of the performance of training programs, but the data showed opportunities for improvement-most importantly, matching current risks and taking one's specific risk profile into consideration. This gap between perceived and actual effectiveness of the training programs hints at more dynamic, responsive training solutions needed that target individual vulnerabilities in a timely and context-specific way. In turn, and in relation to these findings, the present study introduced the Real-Time Behavioral Training System (RTBTS), a new protection mechanism that aimed at improving the cybersecurity posture of individuals through the integration of real-time threat detection with adaptive training modules. This approach forms part of the trend for proactive, customized cybersecurity training methods that exceed education but also engage users in their own defense, turning them into active players within fighting social engineering.

However, the study is limited by the method of data collection, relying on self-report responses, and response bias, in which the subjects might inadvertently misjudge their susceptibility or knowledge of social engineering. Additionally, the sample of the survey will not necessarily mirror the larger population in demographic, work, or computer security exposure variables, and these could contaminate the generalizability of the results. These, collectively, suggest the need to conduct more studies using more representative and diverse samples and mixed or observational measures to complement and validate knowledge of psychological vulnerabilities in social engineering.

Hence, this research provides valuable insights into the interaction between psychology and cybersecurity and offers practical advice on how organizations can enhance their defenses against social engineering. Where cyber threats continue to evolve, so too must our strategies to manage them, making sure that cybersecurity measures are relevant in combatting both today's and tomorrow's challenges.

References

[1] N. Akyeşilmen and A. Alhosban. "Non-Technical Cyber-Attacks and International Cybersecurity: The Case of Social Engineering". In: *Gaziantep University Journal of Social Sciences* 23.1 (2024), pp. 342–360. DOI: 10.21547/jss.1346291.

[2] R. Montañez, E. Golob, and S. Xu. "Human Cognition Through the Lens of Social Engineering Cyberattacks". In: *Frontiers in Psychology* (2020). DOI: 10.3389/fpsyg.2020.01755.

[3] M. Zaoui et al. "A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Toward Effective Mitigation Strategies". In: *IEEE Access* 12 (2024), pp. 72224–72241. DOI: 10.1109/ACCESS.2024.3403197.

[4] *A Look-Back on the First Half of the Year: Phishing and Scam Trends Surrounding the Election, the Technology Sector Spike, and Multi-Channel Threats.* Online Report. 2023.

[5] L. Iacono, K. Wojcieszek, and G. Glass. *Q3 2023 Threat Landscape Report: Social Engineering Takes Center Stage.* Online Report. 2023.

[6] UNICC. *UNICC Cyber Threat Landscape Report 2022.* Online Report. 2023.

[7] *60+ Social Engineering Statistics for 2023.* Online Report. 2023.

[8] Z. Wang, L. Sun, and H. Zhu. "Defining Social Engineering in Cybersecurity". In: *IEEE Access* 8 (2020), pp. 85094–85115. DOI: 10.1109/ACCESS.2020.2992807.

[9] M. K. Mishra and K. D. Pandey. "Social Engineering Attacks and Counter Measures: A Comprehensive Analysis". In: *Double International Journal of Advanced Research in Science, Communication and Technology Access* 4.7 (2024). DOI: 10.48175/www.ijarsct.co.in.

[10] A. Naz et al. “A comprehensive survey on social engineering-based attacks on social networks”. In: *International Journal of Advanced and Applied Sciences* 11.4 (2024), pp. 139–154. DOI: 10.21833/ijaas.2024.04.016.

[11] A. Moroz. “The Use of Psychological Manipulation by a Criminal When Interacting with a Child in Cases of Prolonged Corruption of Minors”. In: *Criminalistics and Forensics* 68 (2023), pp. 652–658. DOI: 10.33994/kndise.2023.68.65.

[12] D. Smith et al. *Psychological, social, and health-related factors predict risk for financial exploitation*. Unpublished or online report. 2024.

[13] R. Marmo and R. Marmo. “Social Engineering Using Social Networking Sites”. In: *Encyclopedia of Criminal Activities and the Deep Web*. IGI Global, 2020, pp. 810–822. DOI: 10.4018/978-1-5225-9715-5.ch054.

[14] T. Mokoena, T. Zuva, and M. Appiah. “Analysis of Social Engineering Attacks Using Exploit Kits”. In: *Intelligent Algorithms in Software Engineering*. Ed. by R. Silhavy. Springer International Publishing, 2020, pp. 189–204.

[15] A. A. Abubaker et al. “Social Engineering in Social Network: A Systematic Literature Review”. In: *2023 International Symposium on Networks, Computers and Communications (ISNCC)*. 2023, pp. 1–7. DOI: 10.1109/ISNCC58260.2023.10323826.

[16] D. Steggles. *Social Engineering*. 2001. DOI: 10.54254/2977-3903/2/2023016.

[17] S. Priya, D. Gutema, and S. Singh. “A Comprehensive Survey of Recent Phishing Attacks Detection Techniques”. In: *2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT)*. 2024, pp. 1–6. DOI: 10.1109/ICITIIT61487.2024.10580446.

[18] I. Opirskyy, S. Vasylyshyn, and A. Piskozub. “Analysis of the Use of Software Baits (Honeypots) as a Means of Ensuring Information Security”. In: *Cybersecurity: Education, Science, Technique* 2.10 (2020), pp. 88–97. DOI: 10.28925/2663-4023.2020.10.8897.

[19] N. Y. Conteh and P. J. Schmick. “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks”. In: *International Journal of Advanced Computer Research* 6.23 (2016), pp. 31–38. DOI: 10.19101/ijacr.2016.623006.

[20] S. Lohani. *Social Engineering: Hacking into Humans*. Available online: https://ssrn.com/abstract=3329391. 2019.

[21] S. M. R. Noval et al. “Dumpster Diving Threat in Personal Data Leakage Case In Indonesia”. In: *International Journal of Ethno-Sciences and Education Research* 3.2 (2023), pp. 63–69.

[22] M. Aldossari and A. Albalawi. “Role of Shoulder Surfing in Cyber Security (Experimental Study to the Comparative Framework)”. In: *American Journal of Computer Science and Technology* 6.3 (2023), pp. 102–108. DOI: 10.11648/j.ajcst.20230603.12.

[23] A. Kamruzzaman et al. “Social Engineering Incidents and Preventions”. In: *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. 2023, pp. 494–498. DOI: 10.1109/CCWC57344.2023.10099202.

[24] H. Aldawood and G. Skinner. “An Advanced Taxonomy for Social Engineering Attacks”. In: *International Journal of Computer Applications* 177 (Jan. 2020), pp. 975–8887. DOI: 10.5120/ijca2020919744.

[25] A. Sales, N. Torres, and P. Pinto. “An Overview of Threats Exploring the Confusion Between Top-Level Domains and File Type Extensions”. In: *CODASPY 2024 - Proceedings of the 14th ACM Conference on Data and Application Security and Privacy*. Association for Computing Machinery, Inc, June 2024, pp. 167–169. DOI: 10.1145/3626232.3658641.

[26] F. Femi-Oyewole, V. Osamor, and D. Okunbor. “A Systematic Review of Social Engineering Attacks & Techniques: The Past, Present, and Future”. In: *International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*. Institute of Electrical and Electronics Engineers Inc., 2024. DOI: 10.1109/SEB4SDG60871.2024.10629836.

[27] D. Steggles. *Social Engineering*. 2001. DOI: 10.54254/2977-3903/2/2023016.

[28] Y. Choi. “Social Engineering Cyber Threats”. In: *Journal of Global Awareness* 4.2 (Dec. 2023), pp. 1–12. DOI: 10.24073/jga/4/02/08.

[29] S. A. Duman, R. Hayran, and I. Sogukpinar. "Impact Analysis and Performance Model of Social Engineering Techniques". In: *ISDFS 2023 - 11th International Symposium on Digital Forensics and Security*. Institute of Electrical and Electronics Engineers Inc., 2023. DOI: 10.1109/ISDFS58141.2023.10131771.

[30] Barry Coatesworth. "The psychology of social engineering". In: *Cyber Security: A Peer-Reviewed Journal* 6.3 (Mar. 2023).

[31] A. S. V. Nair and R. Achary. "Social Engineering Defender (SE.Def): Human Emotion Factor Based Classification and Defense against Social Engineering Attacks". In: *2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1)*. 2023, pp. 1–5. DOI: 10.1109/ICAIA57370.2023.10169678.

[32] W. Keil. "Social Security". In: *Enterprise Social for the Java Platform: Shares, Mashups, Likes, and Ways to Integrate Social Media into Your Cloud Native Enterprise Java Applications*. Ed. by W. Keil. Berkeley, CA: Apress, 2024, pp. 63–111. DOI: 10.1007/978-1-4842-9571-7_4.

[33] V. Greavu Serban and O. Serban. "Social Engineering: A General Approach". In: *Informatica Economica* 18.2 (June 2014), pp. 5–14. DOI: 10.12948/issn14531305/18.2.2014.01.