Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

A comprehensive survey on social engineering-based attacks on social networks

Anam Naz [1], Madiha Sarwar [1], Muhammad Kaleem [1,*], Muhammad Azhar Mushtaq [1], Salman Rashid [2]

[1]Department of CS and IT, University of Sargodha, Sargodha, Pakistan
[2]Department of Computer Science, University of Lahore, Lahore, Pakistan

ARTICLE INFO

Article history:
Received 17 December 2023
Received in revised form
10 April 2024
Accepted 12 April 2024

Keywords:
Social engineering threats
Social networks
Psychological manipulation
Countermeasures
Digital security

ABSTRACT

Threats based on social engineering in social networks are becoming a more common problem. Social engineering is a type of attack that relies on trickery and exploiting human psychology to gain access to confidential information or resources. It involves deceptive techniques like phishing, pretexting, and baiting, tricking individuals into revealing sensitive information or performing specific actions. These tactics can lead to unauthorized access to user accounts, identity theft, or the distribution of harmful content. This study offers a detailed review of threats related to social engineering on social networks. It explores various social engineering attacks, the methods used to execute these threats, and measures that can be adopted to minimize the risk of becoming a victim. The research aimed to develop a new, broad classification of social engineering attacks and strategies for responding to them. It also examines the challenges that social engineering poses to algorithms on social media platforms and highlights the need for more research. The study concludes by pointing out the shortcomings of current approaches and suggesting future research directions, stressing the importance of standardized protective measures and increasing awareness among potential victims. This thorough examination improves our understanding of social engineering attacks and encourages the development of innovative solutions and ethical practices, contributing to a more secure digital environment.

1. Introduction

Today's world has become a global village due to the Internet. Social media is a medium between users, joining them, as the communication that arises due to social networks carries the impact of good and bad purposes. An infinite number of communities are working together to steal someone else personal information through hacking (Chetioui et al., 2022) or spreading false news through posts (Saura et al., 2022), so there is a need to raise awareness and protect themselves from such sites to secure users' property. Social engineering assaults can be carried out in a few ways.to get users to provide useful information (Abroshan et al., 2021b). Social engineering is a broad range of terms related to malicious hacking techniques that use human behavior and emotion to steal personal information. It is a building for cybercriminals to trick people by breaking security with their best practices (Almudahi et al., 2022). Psychological manipulation influences people's behavior or obtains confidential information or resources. Cybercriminals often use it to gain access to systems or data. Social engineering attacks typically rely on the victim's trust and gullibility to succeed (Venkatesha et al., 2021). Phishing is a type of cybercrime where the perpetrator tricks victims into giving them money. It poses a serious security risk to society. Several methods and remedies are available today to stop these assaults. It makes them think that the emails are from a legitimate company and target those who are unaware of online threats and Internet security. Phishing attacks were first introduced to find the target's weaknesses (Hijji and Alam, 2021).

The COVID-19 pandemic has established a new global environment, changing the dynamics in this field. The number of individuals utilizing the Internet and associated online activity has expanded dramatically due to the expansion of work-from-home options, virtual classrooms, and online

* Corresponding Author.
Email Address: muhammad.kaleem@uos.edu.pk (M. Kaleem)
https://doi.org/10.21833/ijaas.2024.04.016
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-6407-4178

entertainment (Andrade et al., 2020). According to market experts, worldwide backhaul demand would increase by more than 47 percent of attacks (Kikerpill and Siibak, 2021). Social engineering often employs deceptive methods such as fake identities and impersonation to gain access to sensitive information, systems, or assets to achieve specific objectives. Individuals, businesses, and society are susceptible to social engineering attacks, which can result in significant consequences such as financial losses, damage to reputation, and increased vulnerability to cybercrime (Schneier, 2021). Businesses, media, social interactions, education, and online platforms have all evolved in the twenty-first century. As a result, both the volume and significance of information moving through the digital world have greatly expanded. As a result, more cybercriminal activities have led to data breaches, malware, ransomware, and phishing attempts (Gupta et al., 2023). Both for-profit businesses and governmental institutions have tried to prevent these assaults. As a result, conventional methods like hacking have shown themselves ineffective over the past few years but are still a weakness. One subject that is getting attention is social engineering and its application to any cyberattack (Matyokurehwa et al., 2022). There have been several attempts over the years, each slightly different but all with the same broad idea, to define the phrase "social engineering attack" in literature. This practice is known as "human hacking" (Chng et al., 2022), which is the art of deceiving individuals into disclosing their login information so that you may use it to access networks or accounts.

This study examines the solutions provided by the research community for investigating and detecting scenarios of social engineering attacks. It thoroughly reviews the terminology related to social engineering in different contexts, analyzing perspectives from various authors and detection methods. The research also investigates advanced hybrid generation and selection techniques using models associated with artificial intelligence (AI). Additionally, the study addresses different types of attacks and their impacts on social networks. Through this survey, agents gain insights into network congestion and strategies for managing it. This survey was used to perform a quantitative analysis of selected articles on social engineering attacks, leading to the creation of a classification system that outlines these attacks and their respective countermeasures.

Section 2 provides a detailed description of the data collection and analysis process. Section 3 explores the challenges and limitations of social engineering models. Section 4 introduces the different types of social engineering attacks. The classification, frameworks, and models of social engineering attacks are detailed in Sections 5, 6, and 7, respectively. The article concludes with Sections 8 and 9, which present the conclusion and future research plans, respectively.

2. Research methodology

A systematic literature review was carried out to identify and categorize the best methods for studying attacks based on social engineering on social networks. This review process includes the collection and analysis of existing research using specific evaluation criteria, which provides insights into the current state of knowledge in this particular area of study (Fuertes et al., 2022). The data from primary sources are methodically organized and examined. The completion of a systematic literature review produces a more structured, logical, and robust response to the main research question (Yasin et al., 2019). The focus of this article includes research papers relevant to social engineering attacks, covering elements like methods, models, and frameworks.

2.1. Research framework

Establishing the framework marked the initial phase of this review. The framework comprised a comprehensive plan that guided the entire systematic literature review process, incorporating three key phases: a planning processing phase, a phase for data selection and evaluation, and a phase dedicated to generating results and drawing conclusions.

2.1.1. Research questions

To successfully review a given title, it is imperative to craft specific research queries. These questions developed for the present systematic literature review were as follows:

Q1: What primary frameworks are used to detect social engineering attacks?
Q2: What are the predominant models commonly employed in social engineering attacks?

2.1.2. Search strategy

A detailed and well-organized process is crucial for collecting valuable information within the chosen area. During this phase, a comprehensive search was conducted to identify significant and relevant data from a large array of information. An automated search process was developed to filter data from multiple sources specific to the desired field. Detailed reviews were carried out on research papers, case studies, and bibliographies of pertinent publications. Additionally, websites that offer information on social engineering, including attack challenges, motives, and various error techniques, were thoroughly investigated. To extract pertinent data, the search was performed with consideration for the following parameters:

- Identification of search terms and keywords depends on research questions

- Inclusion of words relevant to the keywords
- Formulation of search strings using logical operators (such as 'AND' and 'OR') between search words

Keywords associated with social engineering attack techniques were carefully chosen, and the search was enhanced to include synonyms for these keywords. In Table 1, logical operators 'AND' and 'OR' were applied between keywords to enhance the precision of the search. The keywords employed in the search for information related to social engineering are discussed in detail.

Table 1: Search strategy with keywords

Search term	Set of keywords
Social engineering-based attacks *	Social engineering attacks on social networks, manipulating individuals in social networks, deceptive tactics in online social interactions
Security threats in social networks *	Security threats in social media, risks of social engineering on social platforms, protecting against social engineering attacks, measures to counter social engineering, protective strategies against manipulation, frameworks for enhancing security against social engineering threats
Human vulnerabilities in social networks *	Human factors in social engineering attacks, exploiting psychological weaknesses in social networks, understanding vulnerabilities in social interactions
Countermeasures for social engineering *	Countermeasures against social engineering in social networks, safeguarding against deceptive tactics, strategies for enhancing social network security, fraudulent methods for manipulation, and tactics used to exploit human behavior in social engineering
Trust and deception in social networks *	Trust issues in online interactions, deceptive practices in social networks, building resilience against trust-based social engineering attacks
Behavioral analysis in social engineering *	Behavioral analysis for detecting social engineering, machine learning for identifying deceptive behavior in social networks, patterns of manipulation in online interactions, human vulnerabilities in social engineering, understanding the role of human behavior, and factors influencing susceptibility to social engineering attacks
Supervised learning *	Supervised learning models for detecting social engineering attacks, training algorithms for recognizing deceptive patterns, leveraging supervised techniques for social network security
Social engineering types *	Social engineering attack categories, forms of social engineering, and classification of social engineering tactics
Social engineering methods*	Social engineering manipulation techniques, strategies for exploiting human trust, psychological methods in social engineering
Social engineering framework *	Frameworks for understanding social engineering, models for analyzing social engineering attacks, and systematic approaches to studying social engineering incidents
Psychological manipulation techniques *	Psychological manipulation in social engineering, methods for influencing human decisions, and psychological tactics employed in social engineering attacks
Trust exploitation strategies *	Strategies for exploiting trust in social engineering, building and breaking trust in manipulation, trust-based methods in social engineering attacks
Awareness and education for social engineering *	Educational initiatives against social engineering, awareness programs for recognizing manipulation, training frameworks for preventing social engineering incidents
Phishing attacks and social engineering *	Phishing as a social engineering method, social engineering through deceptive emails, techniques for identifying and preventing phishing attacks

The asterisk (*) shows that the search will include all words that begin with the string mentioned before the asterisk

This strategy covers a range of keywords and topics that correspond to the use of social engineering review regarding social networks. It is designed to capture literature on the development and application of various models, including methods, frameworks, types, and different approaches, as well as specific technologies, such as algorithms, for identifying and analyzing behaviors indicative of attack dishonesty.

2.1.3. Resources of search

Our preliminary findings were based on esteemed search engines, including IEEE Xplore, ACM, Springer, and Google Scholar, to retrieve data pertinent to this review. During the initial search, fundamental research content related to the core title was sifted through. Subsequently, the identified research papers and conference proceedings underwent a detailed analysis based on a predefined evaluation method.

2.1.4. Initial selection criteria

The initial curation of research and conference articles adhered to specific criteria, including the language mode of the paper, the year of publication, and the relevance of the topic within the targeted domain. For inclusion in research, papers that are written in English were considered. The paper concentrated on research published between 2017 and 2023. The selected articles were required to align with the finding terms outlined in the search methodology.

2.2. Selection and evaluation procedure

Utilizing the beginning of the search criteria, the finding process retrieved numerous research articles and conference papers. Among the identified articles, 200 were initially selected based on titles deemed related to our study. Meanwhile, a closer examination of the abstracts resulted in the refinement of the selection to 100 research papers, ensuring greater relevance. The research article that passed the abstract-based selection underwent a detailed study. The metrics of these research articles were thoroughly assessed, ultimately leading to the final selection of 81 papers for comprehensive review.

Table 2 provides details on the finalized papers, with 50% of the selected papers sourced from IEEE Xplore and Science Direct. Within this subset, the focus was on journal papers, accounting for 79%, and conference papers, constituting 13%.

Table 2: Search results

Literature source	Search	Step 1: Processing	Step 2: Processing	Step 3: Processing	Manual search	Finalized
IEEE Explorer	200	50	32	14	-	14
ACM DL	121	10	8	6	2	8
Science Direct	103	13	10	7	1	8
Springer	50	11	7	6	-	6
Google Scholar	153	50	41	15	1	16
MDPI	14	10	7	6	-	6
Arxiv	18	15	10	3	-	3
DBLP	29	21	5	3	-	3
Elsevier	25	20	8	2	1	3
Wiley	12	10	2	2	1	3
IOP	10	7	5	1	-	1
Total	735	217	135	65	6	71

A comprehensive examination of the texts of the chosen papers aimed to address specific quality measures inquiries in the current research. The research posed the following quality criteria questions:

A. Thorough coverage of the review's topic

- The focus of the first question was on the extensive coverage of attack detection techniques.
- Evaluation: 82% of the 81 selected research papers satisfactorily covered the topic.

B. Verification of selected paper quality

- The quality of selected papers was assessed based on the reputation of the publishing journal and the number of citations.
- Outcome: An 87% result indicated a satisfactory improvement in the overall quality.

C. Adequate answer to research questions

- The third question gauged whether the selected studies sufficiently addressed the questions outlined in Section 2.
- Outcome: A 72% result suggested the studies' adequacy in addressing the major research questions.

The systematic research exclusively extracted the most related articles within the field of topic selection, ensuring alignment with the specified research questions and quality control criteria. Exclusion criteria involved papers that did not sufficiently address the quality control queries and those unrelated to the study topic. Each question received a Boolean 'yes/no' result, with 'yes' denoted as Y = 1 and 'no' as N = 0. Overall, the responses to these quality questions indicated a robust outcome.

Table 2 depicted a multi-stage literature selection process for the research paper, delineating the number of papers identified, screened, and ultimately included from diverse academic databases as follows:

- Literature source: The first column lists the databases where the literature search was conducted: ACM Digital Library (ACM DL), IEEE Xplore, Science Direct, Springer, Google Scholar, and DBLP.
- Search: The number of papers initially found in each database through a keyword search or other search criteria.
- Step 1: Processing: The number of papers remaining after the first round of screening, which might involve removing redundancy, observing titles and abstracts, or following inclusion/exclusion criteria based on relevance.
- Step 2: Processing: The number of papers still considered after a more detailed review, possibly including a preliminary assessment of the content to ensure it aligns with the research topic.
- Step 3: Processing: The count of papers left after an even more rigorous review, which may involve reading full texts and assessing the quality and direct applicability of the research to the topic.
- Manual search: Additional papers are found through manual searches, such as reviewing the reference lists of selected papers or using snowballing techniques.
- Finalized: The final number of papers selected for inclusion in the research paper after all stages of processing and manual search, indicating those that fully meet the research criteria and contribute meaningfully to the research question or hypothesis.

Fig. 1 shows the detailed literature review process across various academic databases for a research paper, indicating the iterative selection of relevant papers.

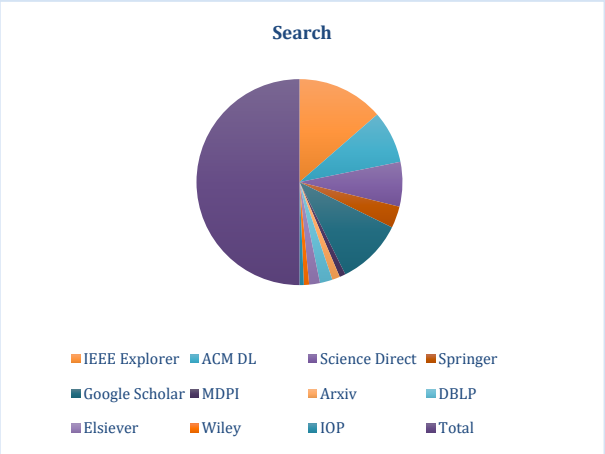

Fig. 1: Searching scaling rate

- IEEE Explorer: Began with 200 searches, refined down to 50 after Step 1, 32 after Step 2, and 14 after Step 3, with no manual search additions, finalizing 14 papers.
- ACM DL: Initially, there were 121 searches, reduced to 10, then 8, and finalized 6 papers after adding 2 from manual searches.
- Science Direct: Started with 103, narrowed to 13, then to 10, with 7 papers finalized post 1 manual search addition.
- Springer: From 50 searches to 11 after Step 1 to 7 after Step 2, with 6 papers finalized.
- Google Scholar: 153 searches were condensed to 50, then 41, with 15 papers finalized including 1 from manual search.
- MDPI: Out of 14 initial searches, 10 were selected, then 6, and 6 finalized.
- Arxiv: From 18 searches, 10 were selected, then 3 and 3 finalized.
- DBLP: Started with 29, reduced to 21, then 3, and 3 papers were finalized.
- Elsevier: Initial of 25 searches, 20 were selected, then 8, with 2 papers finalized after 1 manual search.
- Wiley: Began with 12, down to 10, then 2, and finalized 3 papers.
- IOP: From 10 initial searches to 7, then to 5, with 1 paper finalized.
- Total: The process started with 735 papers across all databases, with 217 surviving Step 1, 135 after Step 2, and 63 after Step 3. Manual searches added 6 more papers, culminating in a final selection of 68 papers for the research. In total, 735 papers were identified across all databases initially, with 81 papers being selected for the final research after all stages of processing and manual searches.

3. Challenges and limitations

The domain of social engineering attacks presents lots of challenges and issues. In this section, we present the most updated challenges. The effect of these challenging mechanisms refers to the psychological and social factors that social engineers exploit to achieve their goals. Human vulnerabilities refer to the weaknesses in human cognition, behavior, and emotions that social engineers exploit. Attack methods refer to the techniques and strategies that social engineers use to manipulate their targets (Wang et al., 2021) as follows:

- Agent training: The tasks agent built vary in difficulty, allow for customization, and gives a mechanism to generate numerous random online hacking problems to train an artificial agent. This can be a particular challenge in the social engineering agent model, as the training data may not be representative of the full range of behaviors and decision-making processes of real individuals. As social networks can be complex and dynamic, agent-based models may not be able to accurately represent all the relationships and interactions between individuals in a network (Erdodi and Zennaro, 2020).
- Looming threats: In actual cases when adequate security protocols have been followed, a single source cannot do substantial damage. Distributed Denial of Wallet will then be examined in combination with current and planned Distributed Denial of Service studies. Despite the widespread impact of social engineering attacks, many individuals and organizations are not aware of the risks and the steps they can take to protect themselves, especially cryptocurrency users (Weber et al., 2020). This makes it easier for attackers to succeed, as individuals and organizations may not be adequately prepared to recognize or resist an attack (Mattera and Chowdhury, 2021; Kelly et al., 2021). Social engineering attacks can have far-reaching consequences, such as financial loss, reputational damage, and increased vulnerability to cybercrime. They can also undermine public trust and confidence in institutions such as banks, government agencies, and online platforms (Kelly et al., 2021).
- Phishing attack algorithm: These algorithms have a flaw in that they have only been applied to Windows XP (Salahdine and Kaabouch, 2019). Most algorithms designed to detect phishing attacks are trained on limited data, making it difficult to detect new and emerging phishing techniques. Additionally, the data used to train these algorithms may not reflect the diversity of phishing attacks that exist in the real world, making it difficult to generalize to all phishing scenarios (Shahrivari et al., 2020; Ansari et al., 2022).
- Scalability: Traditional tactics for detecting phishing attempts are ineffective, detecting just approximately 20% of phishing attacks. ML techniques produce superior results, but at the expense of scalability, they are momentous even on standard datasets. Heuristic strategies for detecting phishing have a significant false-positive rate. ML-based models can require significant computational resources, which can make them infeasible for use in large-scale simulations or real-time monitoring (Anne and CarolinJeeva, 2021).
- URL obfuscation: Phishing attackers may use techniques such as URL shorteners, domain spoofing, or typo squatting to disguise the true destination of a URL. This can make it difficult for link guard algorithms to accurately detect malicious URLs. Attack sources rely on the user interacting with a URL, such as clicking on a link, to initiate a phishing attack [18]. This means that link-guard algorithms cannot prevent phishing attacks that are initiated through other means, such as social media or phone calls. It must consider many variables, such as the source of the email, the content of the email, and the behavior of the user, to accurately detect phishing attacks. This can make it difficult to design algorithms that are

effective across all phishing scenarios (Anne and CarolinJeeva, 2021; Alkawaz et al., 2021).

- Limited data: Algorithms and Models are trained on limited data, and they may not have information about new or emerging phishing domains. This can result in a high rate of false negatives, where phishing attacks are not detected (Almousa and Anwar, 2023). Algorithms can sometimes produce false positives, where they identify a legitimate URL as malicious. This can lead to user frustration and a loss of trust in the algorithm. Phishing attackers may use dynamic content, such as pop-ups or redirection scripts, to redirect users to a malicious URL. This can make it difficult for the detection model to accurately detect and mitigate the true destination of a URL (Madhubala et al., 2022; Abu Hweidi and Eleyan, 2023).

4. Types of social engineering attacks

Social engineering attacks involve deceiving or manipulating individuals to divulge sensitive information or perform actions that allow unauthorized access to computer systems or confidential data. Malicious hackers frequently employ social engineering attacks, employing methods like phishing emails and fake websites to acquire sensitive information or spread malware (Salahdine and Kaabouch, 2019). These attacks manipulate individuals into divulging passwords or private data and can even coerce individuals into sending money or revealing confidential information. By utilizing social engineering tactics, hackers can access valuable resources such as financial data or government records. These attacks are increasingly common and challenging to detect, posing a persistent threat to organizations and individuals. Effective risk mitigation strategies, including awareness of techniques like phishing, pretexting, and tailgating, are essential to safeguard against these attacks (Chetioui et al., 2022; Ahmetoglu and Das, 2022). Further different types of attacks are graphically classified in Fig. 2.

Automated detection of empathy-triggering communication can help prevent social engineering attacks by identifying and alerting potential victims when they are being manipulated. This can be achieved through various techniques, like voice and text analysis, facial expression, and physiological signals, which can identify potential social engineering attacks that aim to manipulate individuals through empathy-triggering communication. Once detected, appropriate warnings or interventions can be triggered to alert the potential victims, thereby helping to prevent them from falling for such attacks. These automated detection methods can contribute to enhancing the overall security posture by providing timely alerts and interventions when individuals are exposed to empathy-triggering communication in various digital and physical contexts (Distler et al., 2023).

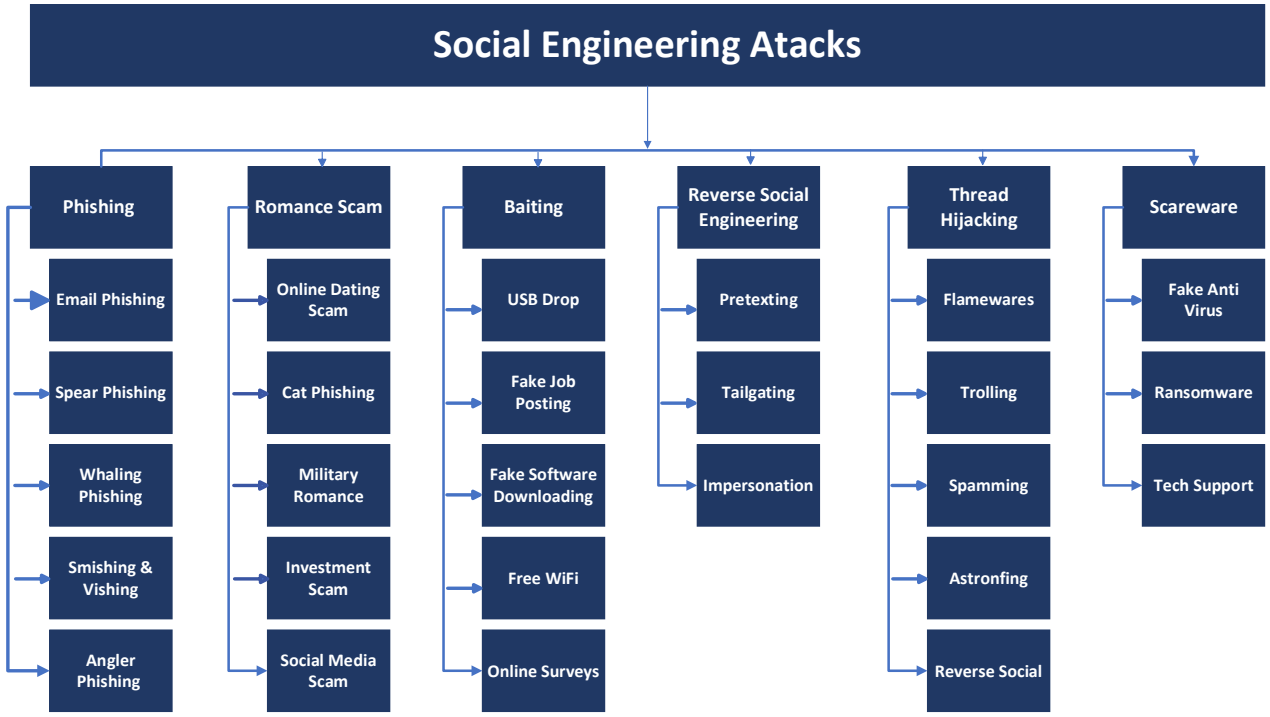

Fig. 2: Social engineering attack types

Social engineering attacks leverage psychological manipulation to deceive individuals or organizations into divulging sensitive information or performing actions that may compromise security. Common methods include phishing, where attackers use deceptive emails or messages to trick recipients into revealing confidential data (Al-Otaibi and Alsuwat, 2020); pretexting, involving the creation of fabricated scenarios or false identities to extract information (Carroll et al., 2022); and

impersonation, where attackers pose as trusted entities to gain unauthorized access. Countermeasures against social engineering attacks encompass robust employee training to enhance awareness and recognition of social engineering tactics. Organizations should implement strict access controls and multi-factor authentication and regularly update security policies. Maintaining a culture of skepticism, where individuals verify requests and report suspicious incidents promptly, adds a layer of defense (Khoei et al., 2022). Technical solutions such as advanced email filtering, endpoint protection, and continuous security audits are also instrumental in mitigating the risks associated with social engineering. Overall, a combination of education, vigilance, and technological safeguards is essential to effectively thwart social engineering attacks (Matyokurehwa et al., 2022).

5. Taxonomy of social engineering attacks framework

By considering elements like the proliferation of threats, the similarities between the assaults, and their individual effects on the characteristics, the suggested taxonomy develops a framework as a specific solution for the social engineering situation. This taxonomy focuses on Mitnick cycle-based vectors of attack propagation. In other words, it focuses on the technique of exploitation rather than the factors from which the vulnerability arises.

5.1. Lifecycle of attack

Social engineering attacks can be conducted in one or more stages and do not need a high degree of cybersecurity skill, as illustrated in Fig. 3. The “investigative phase” of the media manipulation life cycle comprises victim identification, data collecting, and the selection of the optimal attack approach via phishing emails or phone calls (Ahmetoglu and Das, 2022). The second tactic is referred to as a "hook," and it refers to duping the victim(s) to gain ground by influencing the target and dominating the connection. The third step is referred to as "play," during which the attacker carries out the assault and obtains the victim's information. Furthermore, ransomware attacks are launched when the victim clicks on the infected link, which can rapidly spread throughout the victim's network. After an attack by the social engineer, they conclude the relationship by deleting any signs of malware and concealing their trails to prevent discovery.

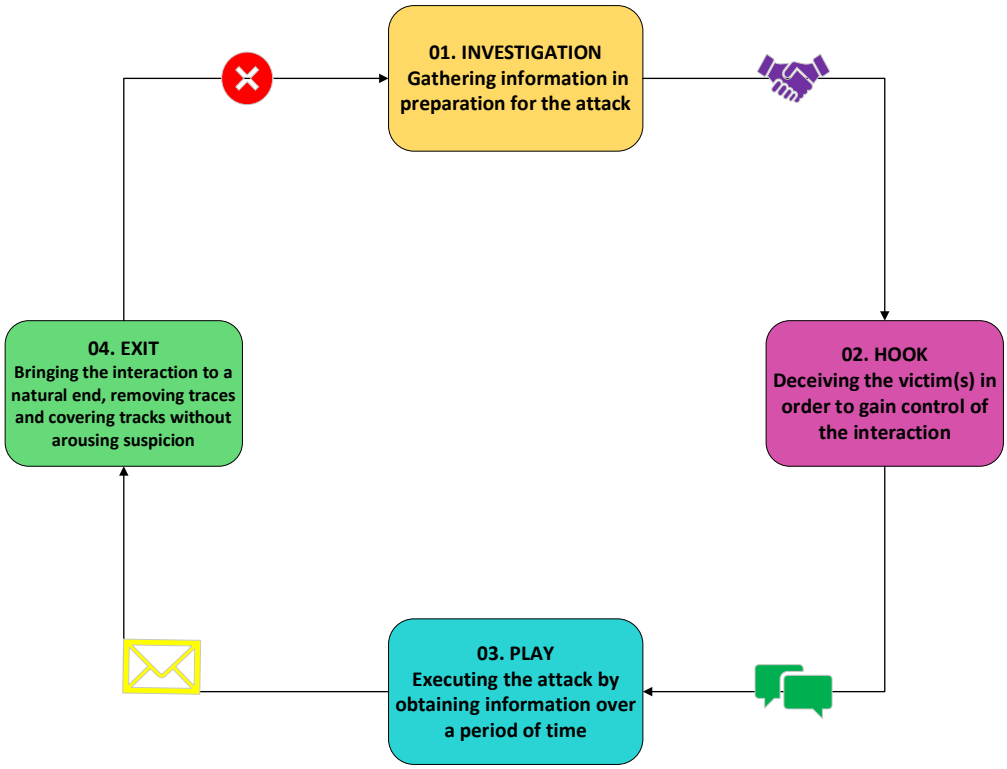

Fig. 3: Lifecycle of social engineering attack formulation

5.2. Kevin Mitnick framework

The framework was created by renowned hacker Kevin Mitnick and provides a comprehensive approach to planning and executing a successful social engineering attack. It emphasizes the importance of research and preparation to maximize the chances of success. It also stresses the need for attackers to be able to identify and avoid security measures, as well as maintain their access over time. This model is based on the idea that social engineering involves manipulating the victim’s psychological processes to gain access to information or resources. It is divided into four stages: gathering information, building trust, exploiting the trust, and obtaining information. The

attacker must be able to gather information about the victim, gain their trust, exploit that trust, and then obtain the desired information or resources. The Mitnick framework is based on direct communication, involving using social engineering tactics to directly interact with the victim and manipulate their behavior (Fatima et al., 2023).

5.3. Enhanced Kevin Mitnick framework

Mitnick's framework uses the major definition of the ontological model to generate a standard map from a historical scenario. The Enhance Mitnick Framework of Social Engineering with the Ontological Model is a conceptual structure that outlines the core elements of social engineering attacks and provides an organized way of identifying and combating such attacks. The framework is based on the work of Kevin Mitnick, a renowned expert in the field of social engineering (Fatima et al., 2023).

The strategies used to manipulate a target are referred to as Tactics or Attack Formulation. Methods of persuasion used to convince a target to take a desired action refer to Information gathering. Before information is provided, there is an additional phase in which the attack goal and the best target to further it are sought. Preparation refers to the items used to facilitate the attack, such as phishing emails and malicious software. To identify the source, Prepare the information that has been obtained and create the assault ploy that will be used during the cyberattack. Prepare the information that has been obtained and create the assault strategy that will be employed during the social engineering attack. Utilize relationship manipulation techniques and preparation to place the target in an appropriate emotional state for the strategy, such as melancholy or happiness, at which point the social engineer should have gotten the information they needed from the target. De-briefing the target entails putting him or her in the desired emotional frame of mind. It is crucial for the target not to feel attacked. The social engineer either concludes during the transition phase that the aim has been achieved or that further information is required, at which point he moves back to the information-gathering phase. The social engineer's first objective of illegal entry has been accomplished to reach the goal (Siddiqi et al., 2022). The Enhanced Mitnick framework is based on both direct communication and indirect communication. It involves researching the target to gain information about their vulnerabilities and potential access points, then directly interacting with the victim to manipulate their behavior and extract the desired data or resources.

5.4. Ontological framework

This model is based on the idea that social engineering involves manipulating the victim's cognitive processes to gain access to information or resources. It is divided into four stages: perception, comprehension, acceptance, and action. The attacker must be able to manipulate the victim's perception of the situation, gain their comprehension of the situation, gain their acceptance of the situation, and then get them to take the desired action. The ontological model is based on indirect communication, as it involves manipulating the victim's cognitive processes without direct interaction (Wang et al., 2021). One social engineer, one target, one or more compliance principles, one or more techniques, one or more mediums, and one goal are all shown in this model. An ontological model adds further structure to characterize this domain. It depicts each entity involved in an assault and the connections between them (Rastenis et al., 2020; Syafitri et al., 2022).

5.5. Personality traits framework

Eliminating attacker profiles and concentrating on human targets are critical beneficiary targets. The victim's capacity to withstand the manipulation of behavior, either by recognizing and/or responding in an attack-coping way, is what determines the success of SE assaults (Kilavo et al., 2023). Investigating Cialdini's concepts of influencing current social engineering research methodologies provided ideas for probable relationships between the Five-Factor Models personality factors (the "Big 5"). The "Social Engineering Personality Framework" (SEPF) is a theory-based work. The Five-Factor Model (Big5) of Social Engineering gave the five factors (Abroshan et al., 2021a). The first step involves using social skills to build relationships and gain trust, which is referred to as extraversion. Agreeableness involves using charm and flattery tactics to gain the victim's trust. By involving consciousness, attackers use patience and strategy to gain access to information or resources. Then, neuroticism involves exploiting the victims' fears and anxieties to manipulate them. Lastly, openness involves using creativity and imagination to gain access. The personality model of social engineering is based on direct communication (Sui et al., 2022), as it involves using persuasive language and tactics to directly interact with the victim and influence their decision-making (Eftimie et al., 2022).

5.6. Phishability traits in human behavior framework

This study was conducted to determine the root causes of phishing, strengthen preventative measures, and suggest mitigation solutions for each stage of the phishing process. Four hypotheses were used to categorize the study model, effects of decision-making style, demographic characteristics, and risk-taking domain (Sadqi and Maleh, 2022). An experimental framework was used to play a risk-taking game and respond to inquiries posed by two psychological measures to assess their behaviors. The perishability of the three phishing phases chosen was then assessed using a mock phishing push. It was discovered that the user's perishability

in the various processes may be predicted by their risk-taking attitude and gender. The findings of this study and the model that was suggested can be utilized to establish a thorough framework for stopping the success of phishing efforts by addressing their underlying causes (Odemis et al., 2022).

To compare all frameworks, the modified and proposed steps of the framework based on those factors through which the social engineering attack occurs through human behavior are shown in Fig. 4. They are manipulating the victim into believing that the attacker is in a position of authority, such as a law enforcement officer or a technician from a tech support company. The attacker gathers information about the target, such as their habits, likes, dislikes, and the company they work for. Intimidation involves implied or direct threats to coerce the victim into providing access or information. Scarcity involves creating a false sense of urgency or limited availability to compel the victim into taking immediate action. Familiarity involves using the victim's personal information or creating a false sense of familiarity to gain trust. Trust involves exploiting the victim's trust to gain access to information or resources. The attacker makes initial contact with the target through email, phone calls, or in-person interactions. Curiosity involves creating curiosity to get the victim to click on a malicious link or take some other desired action. Flattery involves complimenting the victim to gain their trust or manipulate them into taking a desired action. False identity involves creating a false identity and then using it to gain the trust of the victim. These are all the variables that frameworks use to collect data and exploit relationships. The classification of social engineering detection methods is presented in Table 3.

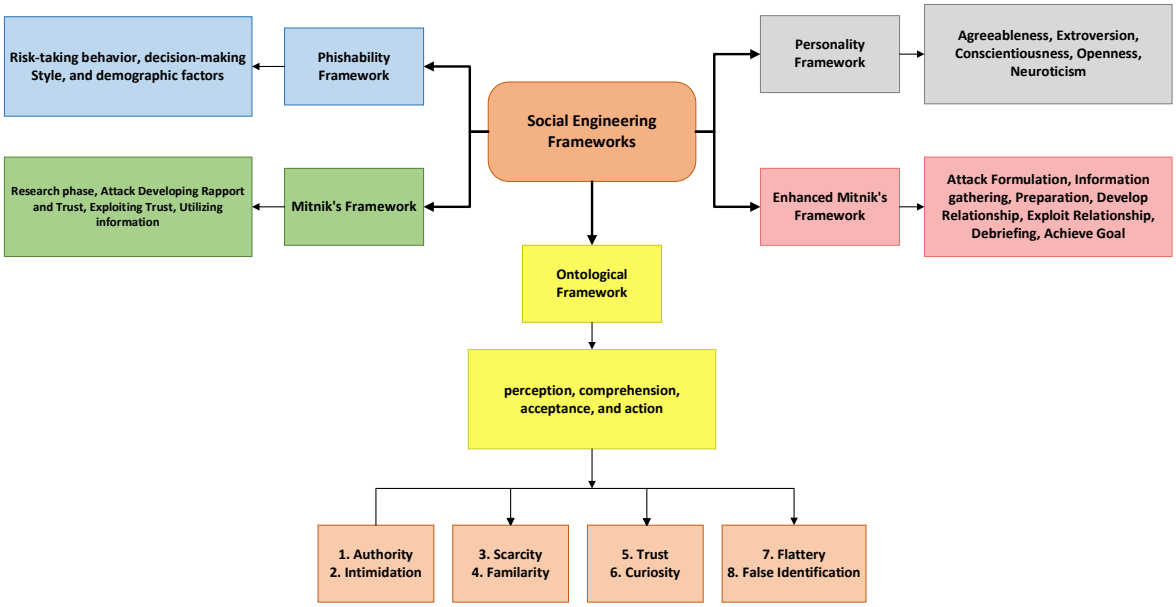

Fig. 4: Taxonomy of different frameworks based on social engineering

Table 3: Classifications of social engineering frameworks

Framework	Criteria	Based on	Mode status		Result
			Direct mode	Indirect mode	
Mitnick Framework (Abu Hweidi and Eleyan, 2023; Fatima et al., 2023)	Security principles and practices	Research phase, attack, developing rapport and trust, exploiting trust, utilizing information	✓	✗	Provides a basic structure that improves system security and reduces the risk of malicious activities
Enhance Mitnick (Abu Hweidi and Eleyan, 2023; Fatima et al., 2023)	Time and flow components	Comprehensive attack lifecycle from goal formulation to debriefing	✓	✓	Addresses shortcomings in the Mitnick attack cycle, enhancing the original framework
Ontological model (Abu Hweidi and Eleyan, 2023; Syafitri et al., 2022)	Domain knowledge, operational knowledge	Stages including perception, comprehension, acceptance, and action	✗	✓	Organizes data and knowledge, providing a foundational system for storage and retrieval
Personality framework (Eftimie et al., 2022)	Personality model, the user interface, the data sources	The Big Five personality traits (extraversion, agreeableness, conscientiousness, neuroticism, openness)	✓	✗	Utilizes the Five-Factor Model and theories of influence to develop strategies in social engineering defense focusing on human factors
Phish-ability model on human behavior (Odemis et al., 2022)	Surveys and questionnaires	Risk-taking and decision-making styles	✗	✗	Aids in designing education and awareness programs to improve individual resilience against attacks
Social engineering attack detection model: SEADMv2 (Abroshan et al., 2021a)	This model was revised to meet both regular and unique needs	Interactions among the request, receiver, requester, and third party	✓	✓	Enhances defense capabilities against social engineering attacks, encouraging a reevaluation of all requests

6. Taxonomy of social engineering attack models

In recent literature, attack models were presented by using Machine Learning Models and Algorithms to detect and mitigate the victim's attack of Agent Web Model, Hybrid Model, Link Guard Algorithm, GBDT, ReDoS, and XGBoost. Social Engineering Model techniques are shown in Fig. 5.

6.1. Agent web model

Agent Web Model system based on machine learning algorithms. This model consists of three main components: the social engineer (the attacker), the target, and the agent. Understanding this model can assist individuals and organizations in recognizing and defending against these types of attacks (Lefoane et al., 2022). Social Engineers can manipulate ML algorithms that can be further used to analyze the behavior and tactics of known social engineers to identify patterns and predict their future behavior. This information can be used to create an AI-powered system that can detect and prevent social engineering attacks. To make active targets, ML algorithms can be used to analyze the behavior and characteristics of potential targets and identify those who may be more susceptible to social engineering attacks. This information can be used to create targeted and personalized attack strategies. Finally, the agent involved ensures that ML algorithms can be used to analyze the communication patterns and tactics used by the agent to identify any suspicious activity. This information can be used to create an AI-powered system that can detect and prevent social engineering attacks carried out through the agent. There is no specific tool designed solely to deploy the Agent Web Model of social engineering. However, TensorFlow can be used to develop and deploy AI models for social engineering detection and prevention (Erdodi and Zennaro, 2020).

6.2. Hybrid model

The Hybrid State-of-the-Art Model of Social Engineering is a framework that combines the strengths of various existing models and approaches to create a comprehensive and effective solution for detecting and preventing social engineering attacks.

This model combines the Agent Web Model, Machine Learning Algorithms, Social Engineering Taxonomy, and Human Factor Analysis. The various components of the Hybrid State-of-the-Art Model are integrated to create a comprehensive solution for detecting and preventing social engineering attacks. The Agent Web Model provides a framework for understanding the relationships between the various components involved in these attacks, while machine learning algorithms and social engineering taxonomy are used to analyze and detect these attacks. Human factor analysis is used to understand how individuals behave and respond to these attacks and to develop more effective defenses (Alkawaz et al., 2021; Huseynov and Ozdenizci Kose, 2022).

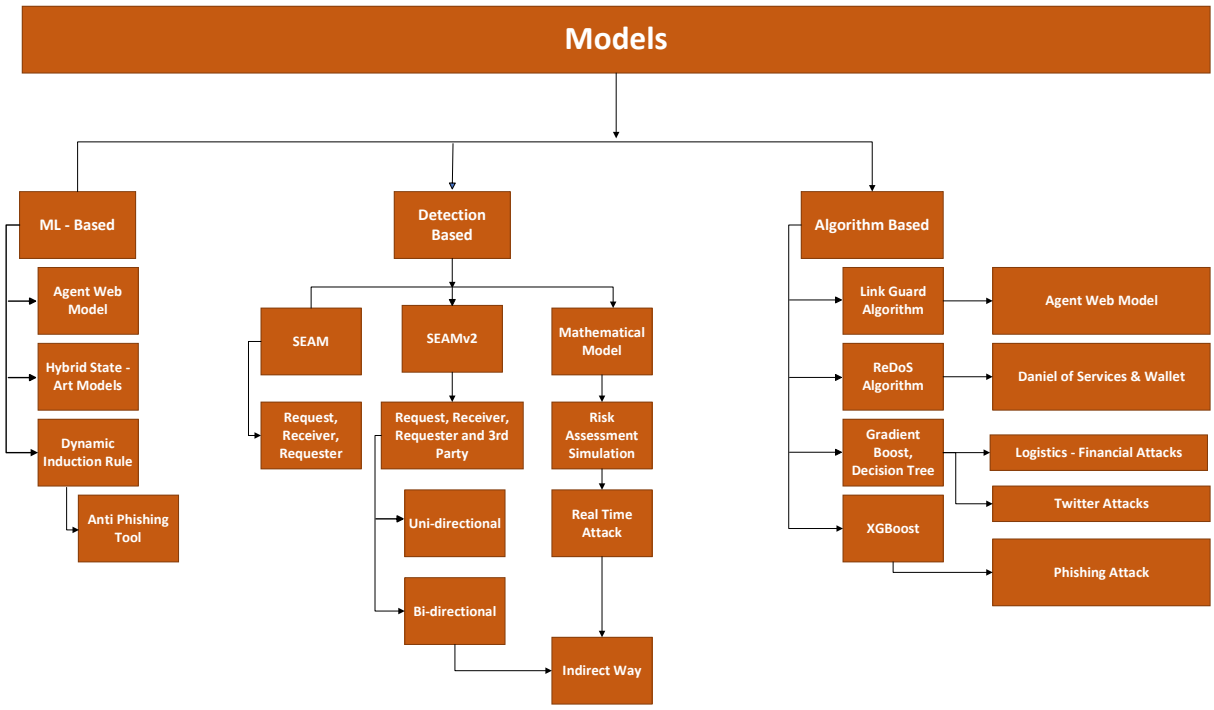

Fig. 5: Taxonomy of models on social engineering

6.3. Link guard algorithm

The Link Guard Algorithm with Machine Learning (ML) is a security solution that is designed to protect against social engineering attacks. The algorithm uses ML techniques with the Agent Web Model to analyze the content of a link and determine whether it is malicious or not (Erdodi and Zennaro, 2020).

This helps to protect users from falling victim to phishing scams, malware downloads, and other malicious activities that can result from clicking on a suspicious link. By using ML to analyze the content of a link, the algorithm can quickly and accurately identify potentially harmful links and prevent users from accessing them. This helps to reduce the risk of users falling victim to social engineering attacks and helps to ensure that sensitive information remains protected (Al Salti and Zhang, 2022).

6.4. Regular expression denial of services

The ReDoS (Regular Expression Denial of Service) Algorithm is a technique used to prevent denial-of-service (DoS) attacks that exploit vulnerabilities in regular expressions. These attacks can be used in the context of social engineering, for example, to cause a server to become overwhelmed with traffic, leading to a crash or slowdown. The purpose of the ReDoS Algorithm is to prevent regular expression-based attacks by analyzing the regular expressions used in an application and identifying those that are vulnerable to ReDoS attacks (Kelly et al., 2023; Eftimie et al., 2022). The algorithm used various techniques to detect these vulnerabilities. Once a vulnerability is identified, the ReDoS Algorithm takes appropriate action to mitigate the risk, such as blocking the regular expression or modifying it to prevent future attacks. This helps to ensure that the application is not vulnerable to social engineering attacks and remains available and responsive to users (Syafitri et al., 2022)

6.5. Gradient boosting decision tree

Gradient Boosting Decision Tree (GBDT) is a ML algorithm that is commonly used for classification and regression problems. To develop a predictive model that can accurately identify malicious activities, such as phishing scams, malware downloads, and other forms of social engineering. GBDT algorithms are trained using large datasets of labeled examples related to Twitter data, and they are about fake account detection. The algorithm uses this training data to learn the characteristics of malicious and benign activities and develops a model that can be used to make predictions on new, unseen data (Shahrivari et al., 2020; Carroll et al., 2022). The GBDT method may be used to examine many forms of data in the context of social engineering, such as email content, Website content, and network traffic, to identify and prevent attacks (Neelakandan and Paulraj, 2020). This helps to protect users and organizations from the consequences of falling victim to social engineering attacks and helps to ensure that sensitive information remains secure (Sharma et al., 2022).

6.6. eXtreme gradient boosting

XGBoost (eXtreme Gradient Boosting) is a powerful machine-learning algorithm that is commonly used for classification and regression problems. It can be applied in the context of social engineering to detect and prevent attacks (Al Salti and Zhang, 2022).

This developed a predictive model that can accurately identify malicious activities, such as phishing scams, malware downloads, and other forms of social engineering. The algorithm works by constructing a grouping of decision trees, where each tree is used to make predictions based on the input data. The predictions from each tree are combined to produce a final prediction, which is used to identify malicious activities (He et al., 2022). Classifications of ML-based social engineering models and algorithms are presented in Table 4.

Table 4: Classifications of ML-based, social engineering models and algorithms

Model	Classification metrics	Feature extraction
Agent web model (Erdodi and Zennaro, 2020)	Reinforcement learning Web hacking → CTF → game → RL problem Abstraction layers: Link, data, dynamics content layer	Websites vulnerabilities
Dynamic rule induction (eDRI) (Aldawood and Skinner, 2020)	Support vector machine (SVM), random forest (RF), neural networks (NN), Naïve Bayes (NB), and logistic regression (LR)	Anti-phishing tool
Stacked auto encoder (SAE) (Kelly et al., 2023)	DDos	traffic from a cloud platform
Tool – Scanner (Pandey et al., 2022)	Software application for testing	Protecting organizations from social engineering attacks
Anomaly detection (DAS) (Chng et al., 2022)	No labeled and nonparametric data; blank profiles	Spear phishing attacks
Link guard (Al Salti and Zhang, 2022)	Identify Harmful links	Link classifications, URL reputation, domain name system analysis
ReDoS (Syafitri et al., 2022)	Uses techniques to detect attacks like; Time complexity, pattern decisions, Heuristics	Target victim variable with multi-dimensional
XGBoost (He et al., 2022)	Predictions based on the input data and deal with a large dataset to detect malicious attacks	Feature engineering, interactions, Handling missing values
GBDT (Sharma et al., 2022)	Analyze website content	Demographic information, technology usage, online behavior, attitudes and beliefs, cognitive biases. These are transformed and processed to create a set of feature vectors that can be used to train the GBDT model

7. Taxonomy of social engineering attack methods

To build a model for learning-based detection and provide scenario-based prediction to guarantee that the data at hand includes phishing and authentic website classes. Many methods are utilized to identify a phishing attempt. Previous research indicates that detecting strategies are employed. Several feature selection strategies are used to decrease features. Classification of social engineering detection methods is presented in Table 5.

7.1. SEAM

SEAM focuses on three main stages of a social engineering attack: preparation, delivery, and exploitation. It defines a set of factors that influence the success of each stage, such as the attacker's motivation, the victim's level of awareness, and the technical proficiency of the attacker. Social Engineering Awareness Model/Security Expertise Assessment Measure consists of a set of questions that measure an individual understanding of social engineering tactics, such as phishing, baiting, and pretexting.

The questions are designed to evaluate both technical knowledge, such as the ability to recognize a phishing email, and behavioral knowledge, such as the importance of keeping personal information confidential (Sánchez-Paniagua et al., 2022).

7.2. SEAMv2

SEAM SEAMv2 builds on the original SEAM framework method by incorporating additional factors, such as the attack vector (e.g., phishing email, phone call), the type of information the attacker is seeking (e.g., personal data, login credentials), and the victim emotional state (e.g., stress, fatigue) (Abroshan et al., 2021a)

7.3. Mathematical model

Social engineering risk assessment simulations are mathematical models designed to evaluate the potential risks associated with a particular social engineering attack. The simulation uses mathematical and statistical methods to model the behavior of the attacker and the potential targets, as well as the impact of the attack on the target systems, data, and processes (Şandor et al., 2022). The goal of these simulations is to provide organizations with a more comprehensive understanding of the potential risks posed by social engineering attacks so that they can take appropriate steps to mitigate or prevent them. This may involve improving their security awareness training programs, enhancing their technical security controls, or developing more effective incident response plans (Pandey et al., 2022).

Table 5: Classifications of social engineering detection methods

Model	Classification metrics
SEAM (Sánchez-Paniagua et al., 2022)	Preparation, delivery, and exploitation, set of questions
SEAMv2 (Abroshan et al., 2021a)	Preparation, delivery, and exploitation, set of Questions, vector attack, the flow of actions
Mathematical model (Pandey et al., 2022)	Analyzing risk vectors through the link

8. Case studies and recommendations

Enhancing the study with a few case studies in real-time that concrete instances strengthen the findings and recommendations, providing a more robust and practical understanding of the dynamics surrounding social engineering attacks in the context of social networks. Moreover, the inclusion of such concrete evidence can serve as valuable illustrations to support the study's key findings and enrich the recommendations. It provides readers and stakeholders with tangible insights into the impact of social engineering attacks and, more importantly, offers practical guidance on mitigating risks and bolstering defenses in the face of evolving threats.

8.1. Case study 1: Phishing campaign exploiting social media trust

In this real-world example, a cybercriminal orchestrated a phishing campaign targeting users of a popular social networking platform (Al-Otaibi and Alsuwat, 2020). The attacker created a fake account impersonating a well-known organization and initiating friend requests and messages to unsuspecting users. The message contained links to a fraudulent website mimicking the social network's login page (Albladi and Weir, 2020). Unwary users, trusting the apparent legitimacy of the sender, clicked on the provided links and entered their login credentials on the fake website. The attacker successfully harvested a significant number of usernames and passwords. Subsequently, the compromised accounts were used to spread malicious links and phishing messages to victims' contacts, perpetuating the attacks. This case highlights the exploitation of trust within social networks and the effectiveness of phishing tactics in compromising user credentials (Gomes et al., 2020). It underscored the need for user education on recognition and verifying communications within social platforms to prevent falling victim to such social engineering attacks.

8.2. Case study 2: Business email compromise on social collaboration platform

In this real-world case, a company heavily relied on a popular social collaboration platform for internal communication and product collaboration. An attacker, after conducting a reconnaissance of the company's employees and their roles, identified a

key executive responsible for approving financial transactions. The attacker then crafted a convincing phishing e-mail, appearing to be from a trusted colleague, and sent it to the executive's social Collaboration platform account. The email contained a seemingly urgent request for a fund transfer to a purported vendor's account. Due to the urgency and the perceived legitimacy of the request coming from a known colleague, the executive approved the transaction. The attacker successfully manipulated the social collaboration platform's messaging system to execute a business email compromise, leading to financial losses for the organization. This case underscores the vulnerability of internal communication platforms to sophisticated social engineering attacks and highlights the importance of implementing robust security measures, including user awareness training and secure communication protocols (Al-Musib et al., 2023).

8.3. Case study 3: Social engineering in influencer marketing

In the context of social networks used for influencer marketing, a real-world example involves an influencer collaboration scam. An attacker created a fake influencer profile, imitating a popular content creator, and reached out to reputable brands for collaboration opportunities. The imposter provided fake engagement metrics, including follower count and engagement rates, to deceive the brands. Several brands fell victim to the scam and agreed to pay for sponsored content or product endorsements. The attacker not only exploited the trust that brands place in influencers but also damaged the reputation of the legitimate influencer whose identity was stolen. This case highlights the risks associated with social engineering in the influencer marketing space, emphasizing the need for brands to verify the authenticity of influencers and implement stringent vetting processes before entering collaborations. It also underscores the importance of influencer education and awareness regarding potential identity theft and scams (Ivanov et al., 2021).

In crafting a review article focused on practical, actionable recommendations for combating social engineering attacks. This includes the development of customized training modules enriched with real-world scenarios, case studies, and interactive elements to engage employees effectively. The establishment of continuous security awareness campaigns, utilizing various communication channels, helps reinforce key security principles and maintains a vigilant workforce. Dynamic password policies should be implemented, emphasizing complexity and regular updates while encouraging the use of password management tools. The promotion of secure communication platforms with end-to-end encryption ensures that sensitive information and transactions are conducted securely. Multi-factor authentication (MFA) solutions, designed for user-friendliness, should be widely adopted, with clear guidance provided on their setup and usage (Mohammed et al., 2023). Collaborative incident response planning involving cross-functional teams and tabletop exercises ensures a coordinated and efficient response to social engineering incidents.

Industry experts recommend a combination of technical solutions and raising awareness among end-users as effective methods to mitigate social engineering risks. The study emphasizes that while technical solutions are necessary, they are not sufficient on their own. Raising awareness and enhancing the information security culture through training is crucial in mitigating the threat of social engineering. Some specific solutions suggested by experts include staff training to recognize phishing attempts, strong security policies, and custom anti-phishing solutions to detect suspicious emails containing unknown links or requests for information from social engineers. Furthermore, updating technical tools is also recommended to help mitigate threats and close security gaps (Aldawood and Skinner, 2020).

Security audits should include a focus on social engineering assessments, analyzing cognitive user behavior and susceptibility to tailor security measures accordingly. Encouraging reporting through anonymous mechanisms and fostering a positive culture of collective security responsibility are critical components of a robust defense strategy (Montañez et al., 2020). Third-party risk management frameworks should be developed to include social engineering risk assessments, with regular reviews of security standards for third-party vendors. Investing in adaptive security technologies, such as those leveraging AI and ML, enhances detection and response capabilities against evolving social engineering tactics. Establishing secure mobile device policies (Mihretu et al., 2023) and implementing mobile device management solutions are vital for protecting against mobile-based social engineering attacks (Weichbroth and Łysik, 2020). Finally, the continuous evaluation and improvement of security measures through metrics, incident response reviews, and user feedback are essential for refining the organization's defenses against social engineering. By emphasizing these practical and actionable recommendations, organizations are seeking to proactively address the dynamic challenges posed by social engineering attacks and fortify their cybersecurity defenses.

9. Discussion and future directions

A social attack involves deceitful tactics aimed at gathering sensitive information such as usernames and passwords through social networking strategies, manipulating human emotions and the tendency to obey instructions. Phishing, a prevalent form of social attack, has become a routine concern online due to its widespread nature and the continual evolution of methods by attackers to deceive users. The previous section offers a detailed comparison of

earlier efforts using diverse methodologies to tackle this issue. Historically, ML techniques, framework-based models, and detection algorithms have been applied to mitigate these attacks. A comprehensive analysis indicated that ML techniques are the most commonly used and effective methods for detecting social attacks. Classification algorithms like SVM, RL, and NB were utilized. Techniques that reduce data features generally enhance performance.

Furthermore, classifications in frameworks are executed using bidirectional, unidirectional, or indirect methods. In terms of algorithm selection, tools like Link guard and XGBoost have identified phishing attempts with moderate success. Defense strategies thus far have primarily focused on human behavior and emotions. Despite a lack of awareness, individuals continue to interact with deceptive URLs, driven by curiosity. To lessen the risk of phishing scams, organizations should focus on diverting employees from core operations and educate them on the dangers of accessing unfamiliar links and webpages.

Future work will focus on establishing and standardizing control problems at higher levels of the classification algorithm. This review expects that the formalization described in this study will not only enable the building of bots but will also raise victim awareness of such assaults, aiding in the process of ethical testing and promoting communication and innovation in both sectors of ML and data security. As the landscape of social engineering and cybersecurity continues to evolve, future research directions are poised to address emerging trends and technologies, offering innovative solutions to combat increasingly sophisticated threats. One prominent area of exploration involves the integration of AI and ML algorithms to enhance the detection and mitigation of social engineering attacks. Researchers are expected to delve into developing advanced models capable of identifying subtle patterns in human behavior, thereby improving the accuracy of threat detection. Moreover, with the proliferation of Internet of Things (IoT) devices, there is a growing need for research focusing on the security implications of these interconnected systems, particularly in the context of social engineering exploits targeting smart environments.

Additionally, as the use of decentralized technologies such as blockchain gains traction, future research may explore their potential in fortifying cybersecurity frameworks against social engineering tactics. The human-centric nature of social engineering also prompts investigations into the psychological aspects of cyber threats, with researchers seeking a deeper understanding of cognitive biases and decision-making processes to design more effective countermeasures.

Lastly, interdisciplinary collaborations between cybersecurity experts and social scientists could yield comprehensive insights into the socio-technical dimensions of social engineering, fostering holistic approaches to safeguarding individuals and organizations against evolving threats.

10. Conclusion

This overview of current attack taxonomies focuses on the functionality and certain attack problems based on frameworks, models, and algorithms taxonomies. Existing attack taxonomies emphasize the distinction between social engineering and technical parts of assaults, which fail to pay adequate attention to confidentiality details and more complex, systematic strategy-based actions. This classification system explains how social engineering attackers focus on authoritative facts and models, using intimidation tactics. It categorizes these factors for clearer analysis. The second node of the taxonomy defines the false news factor spreading by the social engineer to get the target familiar with the confidential data of the victim. This framework is evident, with detailed explanations of each stage, criteria, and category, facilitating a clear understanding. The suggested taxonomy offers a broader set of categorization criteria than previous attack taxonomies based on human behaviors, and the suggested taxonomy provides a more extensive range of categorization criteria than previous attack taxonomies centered on human behaviors. Consequently, the average number of assigned nodes for each attack instance increased, covering aspects like authority, intimidation, scarcity, familiarity, trust, curiosity, flattery, and false identification.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abroshan H, Devos J, Poels G, and Laermans E (2021a). A phishing mitigation solution using human behaviour and emotions that influence the success of phishing attacks. In Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization, ACM, Utrecht, Netherlands: 345-350. https://doi.org/10.1145/3450614.3464472

Abroshan H, Devos J, Poels G, and Laermans E (2021b). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. IEEE Access, 9: 44928-44949. https://doi.org/10.1109/ACCESS.2021.3066383

Abu Hweidi RF and Eleyan D (2023). Social engineering attack concepts, frameworks, and awareness: A systematic literature review. International Journal of Computing and Digital Systems, 13(1): 691-700. https://doi.org/10.12785/ijcds/130155

Ahmetoglu H and Das R (2022). A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. Internet of Things, 20: 100615. https://doi.org/10.1016/j.iot.2022.100615

Al Salti I and Zhang N (2022). LINK-GUARD: An effective and scalable security framework for link discovery in SDN networks. IEEE Access, 10: 130233-130252. https://doi.org/10.1109/ACCESS.2022.3229899

Albladi SM and Weir GR (2020). Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity, 3: 7. https://doi.org/10.1186/s42400-020-00047-5

Aldawood H and Skinner G (2020). Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions. IEEE Access, 8: 67321-67329. https://doi.org/10.1109/ACCESS.2020.2983280

Alkawaz MH, Steven SJ, Hajamydeen AI, and Ramli R (2021). A comprehensive survey on identification and analysis of phishing website based on machine learning methods. In the 11th IEEE Symposium on Computer Applications and Industrial Electronics, IEEE, Penang, Malaysia: 82-87. https://doi.org/10.1109/ISCAIE51753.2021.9431794

Almousa M and Anwar M (2023). A URL-based social semantic attacks detection with character-aware language model. IEEE Access, 11: 10654-10663. https://doi.org/10.1109/ACCESS.2023.3241121

AlMudahi GF, AlSwayeh LK, AlAnsary SA, and Latif R (2022). Social media privacy issues, threats, and risks. In the 5th International Conference of Women in Data Science at Prince Sultan University (WiDS PSU), IEEE, Riyadh, Saudi Arabia: 155-159. https://doi.org/10.1109/WiDS-PSU54548.2022.00043

Al-Musib NS, Al-Serhani FM, Humayun M, and Jhanjhi NZ (2023). Business email compromise (BEC) attacks. Materials Today: Proceedings, 81: 497-503. https://doi.org/10.1016/j.matpr.2021.03.647

Al-Otaibi AF and Alsuwat ES (2020). A study on social engineering attacks: Phishing attack. International Journal of Recent Advances in Multidisciplinary Research, 7(11): 6374-6380.

Andrade RO, Ortiz-Garcés I, and Cazares M (2020). Cybersecurity attacks on smart home during COVID-19 pandemic. In the 4th World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE, London, UK: 398-404. https://doi.org/10.1109/WorldS450073.2020.9210363

Anne WR and CarolinJeeva S (2021). Performance analysis of boosting techniques for classification and detection of malicious websites. In the ICCAP 2021: Proceedings of the First International Conference on Combinatorial and Optimization, European Alliance for Innovation, Chennai, India: 405-415.

Ansari MF, Panigrahi A, Jakka G, Pati A, and Bhattacharya K (2022). Prevention of phishing attacks using AI algorithm. In the 2nd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology, IEEE, Bhubaneswar, India: 1-5. https://doi.org/10.1109/ODICON54453.2022.10010185

Carroll F, Adejobi JA, and Montasari R (2022). How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society. SN Computer Science, 3: 170. https://doi.org/10.1007/s42979-022-01069-1 **PMid:35224514 PMCid:PMC8864450**

Chetioui K, Bah B, Alami AO, and Bahnasse A (2022). Overview of social engineering attacks on social networks. Procedia Computer Science, 198: 656-661. https://doi.org/10.1016/j.procs.2021.12.302

Chng S, Lu HY, Kumar A, and Yau D (2022). Hacker types, motivations and strategies: A comprehensive framework. Computers in Human Behavior Reports, 5: 100167. https://doi.org/10.1016/j.chbr.2022.100167

Distler V, Abdrabou Y, Dietz F, and Alt F (2023). Triggering empathy out of malicious intent: The role of empathy in social engineering attacks. In the Proceedings of the 2nd Empathy-Centric Design Workshop, ACM, Hamburg, Germany: 1-6. https://doi.org/10.1145/3588967.3588969

Eftimie S, Moinescu R, and Răcuciu C (2022). Spear-phishing susceptibility stemming from personality traits. IEEE Access, 10: 73548-73561. https://doi.org/10.1109/ACCESS.2022.3190009

Erdodi L and Zennaro FM (2020). The agent web model-Modelling web hacking for reinforcement learning. ArXiv Preprint ArXiv:2009.11274. https://doi.org/10.48550/arXiv.2009.11274

Fatima A, Khan TA, Abdellatif TM, Zulfiqar S, Asif M, Safi W, Al Hamadi H, and Al-Kassem AH (2023). Impact and research challenges of penetrating testing and vulnerability assessment on network threat. In the International Conference on Business Analytics for Technology and Security, IEEE, Dubai, UAE: 1-8. https://doi.org/10.1109/ICBATS57792.2023.10111168

Fuertes W, Arévalo D, Castro JD, Ron M, Estrada CA, Andrade R, and Benavides E (2022). Impact of social engineering attacks: A literature review. In: Rocha Á, Fajardo-Toro CH, Rodríguez JMR (Eds.), Developments and advances in defense and security. Smart innovation, systems and technologies: 25-35. Volume 255, Springer, Singapore, Singapore. https://doi.org/10.1007/978-981-16-4884-7_3

Gomes V, Reis J, and Alturas B (2020). Social engineering and the dangers of phishing. In the 15th Iberian Conference on Information Systems and Technologies, IEEE, Seville, Spain: 1-7. https://doi.org/10.23919/CISTI49556.2020.9140445

Gupta M, Akiri C, Aryal K, Parker E, and Praharaj L (2023). From ChatGpt to ThreatGpt: Impact of generative AI in cybersecurity and privacy. IEEE Access, 11: 80218- 80245. https://doi.org/10.1109/ACCESS.2023.3300381

He D, Lv X, Xu X, Yu S, Li D, Chan S, and Guizani M (2022). An effective double-layer detection system against social engineering attacks. IEEE Network, 36(6): 92-98. https://doi.org/10.1109/MNET.105.2100425

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: 7152-7169. https://doi.org/10.1109/ACCESS.2020.3048839 **PMid:34786300 PMCid:PMC8545234**

Huseynov F and Ozdenizci Kose B (2022). Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. Information Development, 40(2): 298-318. https://doi.org/10.1177/02666669221116336

Ivanov N, Lou J, Chen T, Li J, and Yan Q (2021). Targeting the weakest link: Social engineering attacks in Ethereum smart contracts. In the Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, ACM, Hong Kong, China: 787-801. https://doi.org/10.1145/3433210.3453085

Kelly D, Glavin FG, and Barrett E (2021). Denial of wallet—Defining a looming threat to serverless computing. Journal of Information Security and Applications, 60: 102843. https://doi.org/10.1016/j.jisa.2021.102843

Kelly D, Glavin FG, and Barrett E (2023). DoWTS–Denial-of-wallet test simulator: Synthetic data generation for preemptive defence. Journal of Intelligent Information Systems, 60: 325-348. https://doi.org/10.1007/s10844-022-00735-3

Khoei TT, Slimane HO, and Kaabouch N (2022). A comprehensive survey on the cyber-security of smart grids: Cyber-attacks, detection, countermeasure techniques, and future directions. ArXiv Preprint ArXiv:2207.07738. https://doi.org/10.4236/cn.2022.144009

Kikerpill K and Siibak A (2021). Mazephishing: The COVID-19 pandemic as credible social context for social engineering attacks. TRAMES: A Journal of the Humanities and Social

Sciences, 25(4): 371-393.
https://doi.org/10.3176/tr.2021.4.01

Kilavo HJ, Mselle LJ, Rais RI, and Mrutu SI (2023). Reverse social engineering to counter social engineering in mobile money theft: A Tanzanian context. Journal of Applied Security Research, 18(3): 546-558.
https://doi.org/10.1080/19361610.2022.2031702

Lefoane M, Ghafir I, Kabir S, and Awan IU (2022). Multi-stage attack detection: Emerging challenges for wireless networks. In the International Conference on Smart Applications, Communications and Networking (SmartNets), IEEE, Palapye, Botswana: 1-5.
https://doi.org/10.1109/SmartNets55823.2022.9994027

Madhubala R, Rajesh N, Shaheetha L, and Arulkumar N (2022). Survey on malicious URL detection techniques. In the 6th International Conference on Trends in Electronics and Informatics, IEEE, Tirunelveli, India: 778-781.
https://doi.org/10.1109/ICOEI53556.2022.9777221

Mattera M and Chowdhury MM (2021). Social engineering: The looming threat. In the IEEE International Conference on Electro Information Technology (EIT), IEEE, Mt. Pleasant, USA: 56-61.
https://doi.org/10.1109/EIT51626.2021.9491884

Matyokurehwa K, Rudhumbu N, Gombiro C, and Chipfumbu-Kangara C (2022). Enhanced social engineering framework mitigating against social engineering attacks in higher education. Security and Privacy, 5(5): e237.
https://doi.org/10.1002/spy2.237

Mihretu AM, Mdumuka J, Shetto M, Rice OP, Iradukunda P, Chamisso TT, and Byiringiro Y (2023). Effective mitigation strategies for social engineering attacks in mobile money services: A case study in Kenya. In the IEEE AFRICON, IEEE, Nairobi, Kenya: 1-3.
https://doi.org/10.1109/AFRICON55910.2023.10293606

Mohammed AHY, Dziyauddin RA, and Latiff LA (2023). Current multi-factor of authentication: Approaches, requirements, attacks and challenges. International Journal of Advanced Computer Science and Applications, 14(1): 166-178.
https://doi.org/10.14569/IJACSA.2023.0140119

Montañez R, Golob E, and Xu S (2020). Human cognition through the lens of social engineering cyberattacks. Frontiers in Psychology, 11: 528099.
https://doi.org/10.3389/fpsyg.2020.01755
PMid:33101096 PMCid:PMC7554349

Neelakandan S and Paulraj D (2020). A gradient boosted decision tree-based sentiment classification of twitter data. International Journal of Wavelets, Multiresolution and Information Processing, 18(4): 2050027.
https://doi.org/10.1142/S0219691320500277

Odemis M, Yucel C, and Koltuksuz A (2022). Detecting user behavior in cyber threat intelligence: Development of honeypsy system. Security and Communication Networks, 2022: 7620125. https://doi.org/10.1155/2022/7620125

Pandey AR, Sharma T, Basnet S, Kumar A, and Setia S (2022). An effective phishing site prediction using machine learning. In the International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), IEEE, Greater Noida, India: 611-616.
https://doi.org/10.1109/ICCCIS56430.2022.10037744
PMid:36006700 PMCid:PMC10152515

Rastenis J, Ramanauskaitė S, Janulevičius J, Čenys A, Slotkienė A, and Pakrijauskas K (2020). E-mail-based phishing attack taxonomy. Applied Sciences, 10(7): 2363.
https://doi.org/10.3390/app10072363

Sadqi Y and Maleh Y (2022). A systematic review and taxonomy of web applications threats. Information Security Journal: A Global Perspective, 31(1): 1-27.
https://doi.org/10.1080/19393555.2020.1853855

Salahdine F and Kaabouch N (2019). Social engineering attacks: A survey. Future Internet, 11(4): 89.
https://doi.org/10.3390/fi11040089

Sánchez-Paniagua M, Fernández EF, Alegre E, Al-Nabki W, and Gonzalez-Castro V (2022). Phishing URL detection: A real-case scenario through login URLs. IEEE Access, 10: 42949-42960.
https://doi.org/10.1109/ACCESS.2022.3168681

Şandor A, Tont G, and Simion E (2022). A mathematical model for risk assessment of social engineering attacks. TEM Journal, 11(1): 334–338. https://doi.org/10.18421/TEM111-42

Saura JR, Ribeiro-Soriano D, and Palacios-Marqués D (2022). Evaluating security and privacy issues of social networks based information systems in Industry 4.0. Enterprise Information Systems, 16(10-11): 1694-1710.
https://doi.org/10.1080/17517575.2021.1913765

Schneier B (2021). Invited talk: The coming AI hackers. In: Dolev S, Margalit O, Pinkas B, and Schwarzmann A (Eds.), Cyber security cryptography and machine learning: Lecture notes in computer science: 336-360. Volume 12716, Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-78086-9_26

Shahrivari V, Darabi MM, and Izadi M (2020). Phishing detection using machine learning techniques. ArXiv Preprint ArXiv:2009.11116.
https://doi.org/10.48550/arXiv.2009.11116

Sharma P, Dash B, and Ansari MF (2022). Anti-phishing techniques–A review of cyber defense mechanisms. International Journal of Advanced Research in Computer and Communication Engineering, 11(7): 153-160.
https://doi.org/10.17148/IJARCCE.2022.11728

Siddiqi MA, Pak W, and Siddiqi MA (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences, 12(12): 6042.
https://doi.org/10.3390/app12126042

Sui Y, Wang X, Zheng K, Shi Y, and Cao S (2022). Personality privacy protection method of social users based on generative adversarial networks. Computational Intelligence and Neuroscience, 2022: 2419987.
https://doi.org/10.1155/2022/2419987
PMid:35463264 PMCid:PMC9020900

Syafitri W, Shukur Z, Asma'Mokhtar U, Sulaiman R, and Ibrahim MA (2022). Social engineering attacks prevention: A systematic literature review. IEEE Access, 10: 39325-39343.
https://doi.org/10.1109/ACCESS.2022.3162594

Venkatesha S, Reddy KR, and Chandavarkar BR (2021). Social engineering attacks during the COVID-19 pandemic. SN Computer Science, 2: 78.
https://doi.org/10.1007/s42979-020-00443-1
PMid:33585823 PMCid:PMC7866964

Wang Z, Zhu H, and Sun L (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9: 11895-11910.
https://doi.org/10.1109/ACCESS.2021.3051633

Weber K, Schütz AE, Fertig T, and Müller NH (2020). Exploiting the human factor: Social engineering attacks on cryptocurrency users. In: Zaphiris P and Ioannou A (Eds.), Learning and collaboration technologies: Human and technology ecosystems: 650-668. Springer International Publishing, New York, USA.
https://doi.org/10.1007/978-3-030-50506-6_45

Weichbroth P and Łysik Ł (2020). Mobile security: Threats and best practices. Mobile Information Systems, 2020: 8828078.
https://doi.org/10.1155/2020/8828078

Yasin A, Fatima R, Liu L, Yasin A, and Wang J (2019). Contemplating social engineering studies and attack scenarios: A review study. Security and Privacy, 2(4): e73.
https://doi.org/10.1002/spy2.73