IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 16 April 2024, accepted 15 May 2024, date of publication 20 May 2024, date of current version 29 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3403197

RESEARCH ARTICLE

A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Toward Effective Mitigation Strategies

MOHAMED ZAOUI[1], BELFAIK YOUSRA[1], SADQI YASSINE[1], (Senior Member, IEEE), MALEH YASSINE[2], (Senior Member, IEEE), AND OUAZZANE KARIM[3], (Senior Member, IEEE)

[1]Laboratory LIMATI, FPBM, Sultan Moulay Slimane University, Beni Mellal 23000, Morocco
[2]Laboratory LISERT, ENSAK, Sultan Moulay Slimane University, Beni Mellal 23000, Morocco
[3]Cyber Security Research Centre, London Metropolitan University, N7 8DB London, U.K.

Corresponding author: Maleh Yassine (yassine.maleh@ieee.org)

ABSTRACT Social engineering (SE) attacks are a growing concern for organizations that rely on technology to protect sensitive data. Identifying and preventing these attacks can be challenging, as they frequently rely on manipulating human behavior rather than exploiting technical vulnerabilities. Although various studies have explored SE attacks and their defense mechanisms, there remains a gap in the literature concerning the holistic and layered classification of these threats and countermeasures. To address this, we conducted a comprehensive literature survey to understand existing taxonomies and subsequently identified areas that required a more structured and exhaustive categorization. Based on the survey results, we propose a comprehensive taxonomy of SE attacks, classifying them based on three levels: environment, approaches, and mediums. Additionally, we present a taxonomy of social engineering countermeasures, encompassing both technical and non-technical solutions. The proposed taxonomies serve as a foundation for future research and offer organizations a valuable framework for developing effective strategies to detect, prevent, and respond to social engineering incidents.

INDEX TERMS Cybersecurity, defense mechanisms, phishing, social engineering, social engineering attacks, social engineering taxonomy, social engineering measures.

I. INTRODUCTION

In today's rapidly evolving and fast-changing digital landscape, safeguarding information systems has become a major concern for individuals and organizations alike. In the pursuit of enhancing security, organizations are increasingly adopting advanced technologies to safeguard their systems and data. While these technical solutions are undoubtedly vital in mitigating potential threats, they alone cannot ensure comprehensive security. However, cybersecurity experts commonly regard the user as the ''weakest link'' in the security chain that receives limited attention. This lack of attention can lead to vulnerabilities that malicious actors can exploit [1], [2], [3], [4]. Considering the relative comparison between technical issues and human mistakes, it is reasonable to describe humans as the most vulnerable aspect of the computer security chain [5]. For instance, despite the development 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 [6]. Furthermore, malicious behaviors such as using weak passwords, clicking on malicious links, sharing sensitive information

The associate editor coordinating the review of this manuscript and approving it for publication was Tiago Cruz.

with unauthorized individuals, downloading infected files, and installing malicious applications can result in security breaches [7]. Individuals utilize Online Social Network (OSN) platforms to interact and communicate for several purposes, such as marketing, entertainment, and business. However, sharing extensive personal details, including ideas, photos, videos, events, and personal information, can expose users to exploitation and privacy concerns [8], [9]. Moreover, the emergence of COVID-19 has led to a shift in the way people live and work, with many organizations moving to remote work and online platforms to continue their operations. Nevertheless, this change has also resulted in an increase in cyberattacks [10]. In recent years, the landscape of cyber threats has evolved significantly, with a notable increase in attacks targeting human vulnerabilities. According to the 2023 Data Breach Investigations Report (DBIR), 74% of breaches result from human errors, privilege misuse, stolen credentials, or social engineering. External actors are involved in 83% of breaches, driven primarily by financial gain in 95% of cases. Attackers commonly gain access to organizations through phishing, pretexting, and system vulnerabilities [11]. This increase in SE attacks indicates that this evolving field requires more attention from both researchers and practitioners [12], [13]. Threat actors are constantly working to identify new tricks and means to trick victims into revealing their sensitive data. Social engineering refers to the practice of manipulating individuals into revealing confidential information, and the act of carrying out this tactic is known as a social engineering attack [14]. These kinds of cyberattacks are extremely successful because they rely on human emotions such as fear, greed, curiosity, rushing, and trust [15], [16]. Although social engineering is commonly associated with manipulating individuals to disclose confidential information, it is imperative to recognize that these attacks can also involve physical access methods, such as piggybacking or strategically placing USB drives in the victim's workplace or parking lot. This highlights the need for organizations to educate employees about the potential risks associated with physical security breaches and implement access control policies to enhance physical security and prevent unauthorized access [14]. People generally believe that they are adept at detecting such attacks. However, research shows that people perform poorly at detecting deceptions [17]. Hackers understand that the easiest method to infiltrate a system or obtain sensitive information is by manipulating individuals into performing actions or revealing confidential data [18]. With unrestricted access to technological tools and the digitalization of communications, the prevalence of psychological techniques employed for harassment, intimidation, threats, and information theft has surged. Despite this, research focused on cybersecurity, particularly concerning social engineering techniques, remains relatively scarce [3]. Cybercriminals choose social engineering techniques when there is no way to infiltrate a system with no technical vulnerabilities [19]. Social engineering attacks have proven to be highly effective in breaching security defenses, compromising sensitive information, and causing significant financial and reputational damage to individuals and organizations [20]. To effectively combat social engineering attacks, it is crucial to understand the underlying techniques and psychological principles employed by attackers [21].

A. RESEARCH MOTIVATION

The growing incidence and complexity of social engineering attacks in our interconnected world have prompted researchers to investigate these malicious activities and develop effective countermeasures. To effectively combat social engineering attacks, it is essential to develop comprehensive taxonomies that categorize these attacks and identify suitable defense mechanisms. The main aim of this research is to develop comprehensive taxonomies of social engineering attacks and defense mechanisms, with a particular emphasis on identifying effective mitigation strategies to enhance cybersecurity. By understanding the various tactics employed by attackers and the corresponding defense mechanisms, we aim to provide valuable insights into the nature of social engineering attacks and equip individuals and organizations with the knowledge and tools necessary to protect themselves against such threats. One of the key motivations for this research is the realization that traditional security measures are often insufficient to combat social engineering attacks. While technological advances have certainly enhanced security in many areas, attackers have shifted their focus to the weakest link in the security chain (i.e., the human element). To address this issue, there is an urgent need to shift the cybersecurity paradigm and place greater emphasis on human-centric risks. This study emphasizes the significance of considering human factors in developing effective security strategies. Attackers can bypass even the most robust technical defenses by exploiting human vulnerabilities such as trust, curiosity, and fear. Furthermore, social engineering attacks are not limited to specific industries or sectors. They can target anyone, from individuals to large companies, and can have severe consequences, including financial loss, reputational damage, and even violations of national security. Therefore, it is crucial to develop an in-depth understanding of social engineering techniques and defense mechanisms to effectively mitigate the risks associated with these threats. Another motivation for this research is the lack of a standardized taxonomy that encompasses a wide range of social engineering techniques and defense strategies. Existing research lacks a comprehensive approach that classifies both social engineering attacks and countermeasures, resulting in a knowledge gap and a lack of a systematic framework for addressing these threats. While the existing research provides valuable insights into the classification and categorization of social engineering attacks [18], [32], [43], [44], [45], [46], [47], comparatively less attention has been given to the development of taxonomies focusing specifically on social engineering countermeasures [61], [62]. Our study aims to

fill this gap by presenting comprehensive taxonomies that address both social engineering attacks and their corresponding countermeasures. This research will provide a practical framework for effective mitigation strategies, contribute to the advancement of knowledge in the field of cybersecurity, and serve as a valuable resource for researchers, practitioners, and policymakers. Additionally, the proposed taxonomies will facilitate the development of tailored training programs and effective security policies, ensuring that organizations are equipped to recognize and respond effectively to social engineering attempts.

B. MAIN CONTRIBUTIONS

Inspired by the above motivations, this paper makes several significant contributions to the field of social engineering attacks and defense mechanisms. The main contributions can be summarized as follows:

- **Comprehensive overview of social engineering:** This paper provides a comprehensive overview of the various social engineering techniques employed by attackers. It explores the tactics used to manipulate individuals and exploit their vulnerabilities. Additionally, the paper presents a detailed examination of the corresponding countermeasures that can be implemented to mitigate the risks associated with these attacks.
- **Multi-layered taxonomy of SE attacks:** One of the key contributions of this paper is the development of a detailed taxonomy of social engineering attacks based on three levels, which are environment, approaches, and mediums.
- **Taxonomy of SE countermeasures:** In addition to the taxonomy of social engineering attacks, the paper proposes a taxonomy of countermeasures that encompasses both technical and non-technical solutions for analyzing, developing, and implementing comprehensive defense strategies that address the unique challenges posed by social engineering attacks.
- **Structured framework:** The paper offers a structured framework that enables the analysis, understanding, and strengthening of defense mechanisms against social engineering threats.
- **Guidance for future research directions:** Lastly, this paper provides valuable insights that can guide future research directions by encouraging researchers to explore other potential levels, dimensions, and aspects to evolve the proposed taxonomy.

C. ORGANIZATION OF THE PAPER

The remainder of this paper is organized as follows: Section II provides an overview of social engineering. Section III describes the research methodology. Section IV analyzes existing taxonomies regarding the social engineering field. Section V introduces our proposed taxonomy of social engineering attacks. Section VI presents a taxonomy of the countermeasures that can be implemented to counter SE threats, focusing on both technical and non-technical solutions. Section VII addresses research challenges and future directions. Finally, Section VIII concludes the paper.

II. OVERVIEW OF SOCIAL ENGINEERING

A. CONCEPT AND STAGES

In the field of cybersecurity, social engineering is a well-known concept that describes a cyberattack technique targeting human weaknesses instead of technical vulnerabilities. This form of cyberattack is often referred to as "the art of people hacking," as it involves manipulating individuals to divulge sensitive information or perform actions that compromise their security [22], [23]. The process of social engineering attacks generally consists of four main stages: information-gathering, establishing a relationship, exploitation, and execution. Most attacks' success hinges on the information-gathering phase's effectiveness, leading attackers to devote considerable time and effort to this initial stage. Attackers frequently begin by exploiting the wealth of publicly accessible information from individuals' online presence, particularly on social media platforms. This information may be employed directly in the execution of the attack or used to obtain further information from secondary sources [24]. Once the attacker has gathered sufficient details on the target, they advance to the relationship establishment stage, focusing on cultivating trust with the target [25], [26]. The exploitation stage aims to accomplish the attack's objective by employing persuasive and manipulative techniques to retrieve sensitive information from the target or mislead them into making security mistakes [27], [28]. Finally, after achieving their malicious goal, the attacker terminates the interaction with the victim and may attempt to cover their tracks by erasing any evidence or traces that could lead to identification or tracking [29]. Fig. 1 shows the different stages of a social engineering attack.

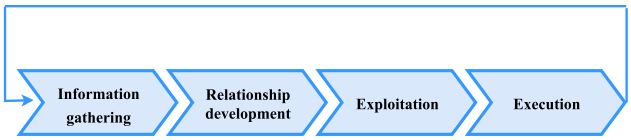


FIGURE 1. Social engineering attack stages.

B. COMMON ATTACKS

Social engineering attacks have no limit, and they only depend on the creativity of social engineers. This section provides a brief description of the different kinds of common social engineering attacks.

1) PHISHING

Phishing is a type of social engineering attack where the attacker disguises himself as a trustworthy entity and creates a fraudulent communication (e.g., an email or text message) that appears to be from a legitimate source to manipulate the recipient into revealing sensitive information, such as login credentials and credit card details, or performing an action that is harmful to their security or privacy. While phishing

attacks are commonly associated with email and VoIP, these deceptive tactics can also extend to other communication channels and mediums, including websites, software, instant messaging apps, and online advertisements. Overall, there are five primary types of phishing attacks: **General Phishing** (the traditional method of phishing), **Spear phishing** (a targeted version of the phishing),**Smishing** (SMS phishing),**Vishing** (voice phishing),**Whaling** (high-profile targets) [19], [30], [104].

2) BAITING

Baiting is a social engineering attack involving enticing a victim with the promise of something desirable or a reward that the target can obtain for free (e.g., a free movie or software). For instance, attackers may leave a malware-infected flash drive at the target's workplace, where the victim might, out of curiosity, insert the device into a computer and infect their system with malware [18], [23], [27], [31].

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 social engineering technique where an attacker offers a service or benefit in exchange for sensitive information or access. For example, an attacker may pretend to be an IT support technician, offering assistance to a victim who may be facing technical challenges that require sensitive information (e.g., login credentials) to be solved [33], [34].

4) WATERING HOLE

The name watering hole attack is derived from a real-life scenario in which the predator lurks near the waterholes, knowing that their targeted prey will eventually come to drink. Similarly, in this attack, the attacker identifies a website that their target frequently visits and infects it with malware. When the target visits the compromised site, they unknowingly download malicious code, giving the hacker access to their system [26], [31].

5) DUMPSTER DIVING

Dumpster diving is a social engineering technique in which an attacker physically searches through a target's trash or discarded materials (e.g., old computer materials, storage devices, CDs) to find valuable information that can be used for malicious purposes. This type of attack can be particularly effective because many people don't realize the importance of properly disposing of documents, papers, and even hardware (i.e., shredding documents or securely erasing digital files) [19], [23], [33].

6) PRETEXTING

This is a form of social engineering where attackers focus on creating a good pretext or a fabricated scenario by impersonating an authority figure or a trustworthy entity, such as co-workers, police officers, bank employees, or tax officials, to gain the victim's trust and trick them into divulging sensitive information or performing actions [19], [23], [26], [33].

7) SHOULDER SURFING:

Refers to using direct observation techniques to collect personal information by looking over someone's shoulder at their screen or keyboard, typically used for extracting authentication data such as PINs, passwords, or other confidential information that can be used for malicious purposes [18], [23], [27], [33].

8) TAILGATING

Also known as ''piggybacking,'' this attack requires physical proximity and involves closely following someone who has authorized access to a restricted area. The attacker may use various tactics, such as posing as a delivery person, pretending to be lost, or simply asking the victim to hold the door, to bypass security measures such as access control systems, ID checks, or security personnel [23], [32], [33].

9) SCAREWARE

A scareware attack is a type of cyberattack that involves tricking users into believing that their computer or mobile device is infected with malware or other security threats. The attacker typically employs pop-up messages or other social engineering techniques to persuade the victim to download and install fake security software [19], [32].

10) REVERSE SOCIAL ENGINEERING

In this form of attack, the attacker creates a situation in which the victim feels the need to contact them for assistance or information. For instance, the attacker might cause a technical issue and then pose as an expert who can resolve it. The victim may then divulge confidential data to the attacker, believing they are interacting with legitimate authority [19], [23].

III. RESEARCH METHODOLOGY

A. RESEARCH DESIGN

Our research methodology relies on the guidelines described by Molléri et al. [35] to conduct survey-based research. This methodology is suitable for our research objectives because it provides a systematic process that helps ensure relevant papers are collected and analyzed in a way that adequately addresses the research questions. Fig. 2 provides a clear overview of the research methodology. It highlights the steps followed in retrieving relevant studies, selecting papers, and conducting a comprehensive analysis.

B. RESEARCH QUESTION

Identifying the research question is the first step, which must be concise and clear. In the context of this study, the aim of this research can be formulated into the following main research questions:

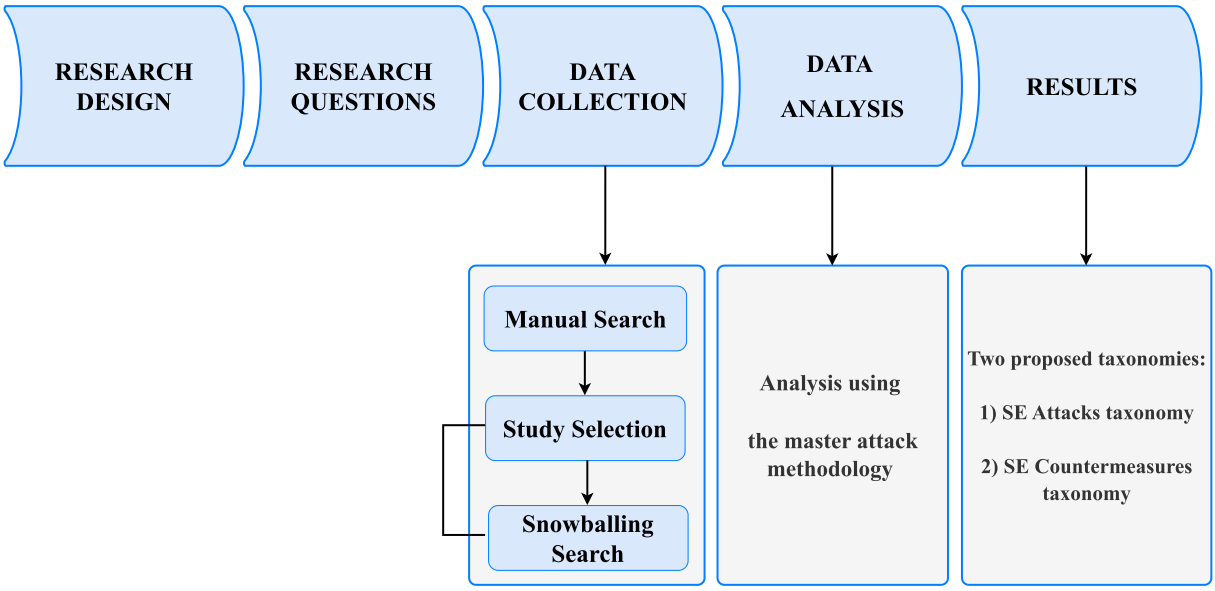


FIGURE 2. Overview of research methodology.

- RQ1: What are the different types of social engineering attacks, and how can they be classified?
- RQ2: What are the effective countermeasures to prevent social engineering attacks, and how can they be classified?
- RQ3: What are the primary research challenges facing researchers and practitioners in the social engineering field?

C. DATA COLLECTION

To retrieve as many relevant studies as possible, we carried out an iterative search and selection process in three steps, starting with manual searches and subsequent categorization of papers. The manual search is then complemented with a backward and forward snowballing technique to identify additional relevant studies. Fig. 3 shows the three phases of the search process used to retrieve relevant primary papers.

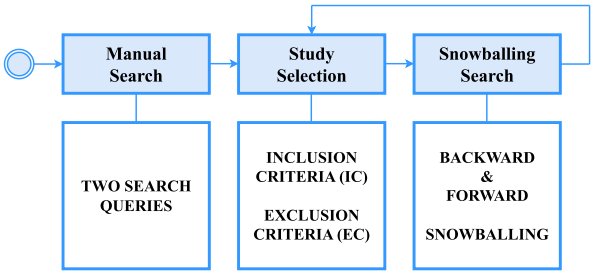


FIGURE 3. Search and selection process overview.

- **Manual Search:** The first set of papers was selected through a manual search on Google Scholar to avoid bias toward any specific publisher. Two search queries (SQ) are pre-defined according to research objectives, employing combined keywords and Boolean operators as follows:
  - **SQ1:**(social engineering AND (attacks OR approaches OR techniques OR classification OR taxonomy OR countermeasures OR mitigation OR defense mechanisms)).
  - **SQ2:**(social engineering AND (challenges OR open issues OR concerns)).
- **Study Selection:** We verified the relevance of each paper by reading the title and abstract and ensuring that they aligned with our research objectives. After collecting the selected papers into a single list, we applied the following inclusion criteria (IC) and exclusion criteria (EC):
  - **IC1:** English is the language of the article;
  - **IC2:** Articles were published between June 2013 and June 2023;
  - **IC3:** Studies supporting survey research in social engineering;
  - **IC4:** Articles addressing SE attacks and techniques;
  - **IC5:** Articles addressing mitigation techniques against SE threats;
  - **IC6:** Papers proposing classifications or taxonomies of SE attacks;
  - **IC7:** Papers proposing classifications or taxonomies of SE defense mechanisms;
  - **IC8:** Papers addressing research challenges and open issues in the social engineering field;
  - **EC1:** Articles that are not written in English;
  - **EC2:** Irrelevant and out-of-scope studies;
  - **EC3:** Duplicate articles that cover the same research or findings.

After applying the selection criteria to 133 downloaded papers from the first research query (SQ1), nine papers were excluded due to duplication, 34 papers were rejected after reading the abstract, and 28 articles were irrelevant and out-of-scope studies. Similarly, after

applying the selection criteria to 16 downloaded articles from the second research query (SQ2), nine papers were available for analysis to identify the challenges facing researchers and practitioners as they encounter this evolving field. The candidate papers were categorized into four main groups: attacks, countermeasures, taxonomies, and challenges.

- **Snowballing Search:** To enhance the coverage of relevant studies, the manual search was supplemented with backward and forward snowballing techniques following the snowballing procedure guidelines described in [36]. For backward snowballing, we examined the reference lists of selected papers, considering the criteria described above. We carefully evaluated the references to determine the relevance of the candidate papers. For forward snowballing, we utilized Google Scholar to study the citations to the paper being examined. We initially screened the candidate citing papers based on the information provided, and if necessary, we conducted a more detailed examination, including reviewing the abstract and full text of the citing papers. Following these practical steps, we analyzed all the remaining 62 papers from the three categories. We identified a total of three relevant papers. However, we excluded four case studies as they did not align with our inclusion criteria. For instance, we excluded studies that did not meet the inclusion criteria (IC2), which specifies a focus on papers published between June 2013 and June 2023.

At the end of this phase, 74 papers were available for analysis, as shown in Table 1.

TABLE 1. Overview of retrieved articles.

Groups	Description	Number of papers
Attacks	Papers primarily discussing various forms of social engineering attacks, their methods, and case studies.	10
Countermeasures	Papers focusing on defense mechanisms, mitigation strategies, and countermeasures against social engineering attacks.	31
Taxonomies	Papers presenting or proposing taxonomies and classifications related to social engineering attacks and defense mechanisms.	24
Challenges	Papers addressing the challenges and open issues in the field of social engineering.	9

D. DATA ANALYSIS

A comprehensive analysis was performed on the collected studies and papers, utilizing the main attack methodology [37]. The Main Attack Methodology is an integrated approach developed to understand and plan the full lifecycle of cyberattacks. It is designed to be scalable across various industries and computing systems, providing a standardized framework for building attack trees. This methodology encompasses four key features: the 'when,' 'where,' 'what,' and 'how' of an attack. The 'when' refers to the phasing sequence of the attack, while the 'where' represents the potential surface area where the attack could occur. The 'what' encompasses the actions and adversarial tactics required to accomplish each phase of the attack. The 'how' refers to the tools and techniques used to execute these actions. In this study, the analysis was structured around the anatomy of an attack, focusing on three key aspects: the "**what**", "**where**", and "**how**" of each attack. "What" refers to the attacker's objective or the intended outcome of the attack. It seeks to answer the question, "What was the attacker's goal?" This could range from stealing confidential data or unauthorized access to causing systemic disruption. The "what" could manifest in various forms, such as a phishing attempt, a baiting attack, or a pretexting scenario. The "what" primarily addresses the question: "What are the prevalent forms of social engineering?". "Where" focuses on the context or environment of the attack. It could refer to the physical or virtual location where the attack was executed. For instance, was the attack conducted in-person or remotely? The "How" examines the methods or techniques employed by the attacker to achieve their objectives. It could be associated with both the approach and the medium used for the attack. For example, was the attack executed via an email scam, a malicious website, or a deceptive phone call? Furthermore, it investigates the specific tactics used within these mediums to deceive the victim. This data analysis section served as the foundation for proposing two taxonomies. The first taxonomy, which classifies social engineering attacks, is the result of an exhaustive analysis of various studies and is structured around three fundamental aspects: the environment, approaches, and mediums (see Section V). Furthermore, a taxonomy of social engineering countermeasures has been introduced, emphasizing technical and non-technical solutions. This taxonomy organizes and categorizes countermeasures into four essential categories, as detailed in Section VI. In addition, a comprehensive analysis of the retrieved papers and case studies has been conducted to identify open issues, emerging trends, and persistent challenges that may face researchers and practitioners in combating social engineering attacks and implementing effective defense mechanisms (see Section VII).

IV. AN OVERVIEW OF EXISTING TAXONOMIES

Taxonomies are hierarchical structures that classify concepts or objects according to their interrelationships or similarities. In the context of research and literature review, taxonomy is essential for organizing and classifying knowledge, providing a structured framework for comprehending complex topics [38]. According to Sadqi and Maleh's [39] review of the works of various researchers, ten requirements have been identified for a satisfactory taxonomy. These requirements include: (1) being based on approved previous works, (2) providing clear and understandable information,

(3) considering all possible attacks and providing well-defined categories, (4) having a clearly defined classification procedure, (5) ensuring mutual exclusivity to avoid overlap, (6) allowing for reproducibility in the classification of attacks, (7) conforming to standards in terminology, (8) using well-defined terms with clear criteria, (9) being unambiguous with clearly defined categories, and (10) being useful in different contexts.

A. TAXONOMIES OF SE ATTACKS

Several researchers have proposed distinct taxonomies to classify social engineering attacks, with each taxonomy focusing on specific aspects or dimensions of these attacks. For instance, Social engineering is traditionally divided into two primary categories: human-based and technology-based [40], [41], [42]. This division highlights the role of human interaction and technology in facilitating social engineering attacks.

In [18], Krombholz et al. proposed a taxonomy to handle the specific challenges posed by the use of communication and collaboration tools in business environments. They classified social engineering attacks based on three main categories: channel, operator, and type. The channels through which social engineering attacks could be performed included email, instant messaging applications, telephone, voice-over-IP, social networks, cloud services, and websites. Two primary operators (humans or software) were responsible for the attack, with software-based attacks offering a higher capacity for reaching a larger number of targets. In addition, the authors categorized social engineering attacks as physical, technical, social, and socio-technical.

In another study [43], the authors conducted a study on social engineering attacks, focusing on their approach and means of communication. They categorized these attacks into interpersonal and non-interpersonal approaches. This research aimed to address the issue of unintentional insider threats (UIT) caused by social engineering exploits by collecting and analyzing data from UIT incidents to identify probable behavioral and technical patterns.

Heartfield and Loukas conducted a research study [44] in which they developed a taxonomy of semantic social engineering attacks. The main objective of their research was to contribute to the understanding of semantic attacks and facilitate the development of effective defense strategies. Their taxonomy aimed to classify semantic attacks based on their core characteristics rather than focusing on specific implementations. This allows for a universally applicable and platform-independent approach, enabling defense measures to be more broadly applicable across various attack types with similar traits.

In their study [45], Koyun and al. Janabi presented a comprehensive overview of social engineering attacks and a taxonomy categorizing them based on their phases, types, approaches, and channels. Information gathering, relationship development, exploitation, and execution are the phases of a social engineering attack. The types of these attacks are divided into human-based and computer-based attacks. The approaches used by attackers include physical, social, technical, and socio-technical. The proposed taxonomy identifies various channels through which social engineering attacks can be performed, including instant messaging applications, email, social networks, physical actions, cloud services, voice-over-IP, and websites.

The authors of [46] analyzed the vulnerabilities present in various personal devices, including mobile devices, desktops, and tablets. They proposed a taxonomy that classifies social engineering attacks based on the specific devices employed. The taxonomy provides valuable insights into the vulnerabilities and attack vectors associated with each device. For instance, mobile devices are susceptible to phishing, Bluetooth phishing, malicious applications, and ransomware attacks. Desktops can be targeted through cloud servers, USB and flash drives, network connections, web browsers, and rootkits. Tablets, on the other hand, are vulnerable to attacks through Wi-Fi and Bluetooth connections, cloud sharing, social networking sites, and outdated software. This study also highlights the importance of linking past and future cases to develop early warning signs for detecting and preventing social engineering attacks.

In [32], the authors highlighted the significance of social engineering attacks in the modern technology and internet era and emphasized the necessity of implementing preventive measures at both the human and technical levels. The proposed taxonomy classifies social engineering attacks according to their types, operators, and mediums of attack. It includes approaches utilized by social engineers, such as social, technical, socio-technical, physical, in-person interaction, and technology-based interaction.

The authors of the study [47] made a clear distinction between human-based and computer-based social engineering attacks by presenting a classification based on three main categories: operator (human-based and computer-based attacks), methods of deception (social-based, technical-based, and physical-based attacks), and nature of communication (direct and indirect communication attacks). In addition to highlighting the limitations and challenges faced in countering social engineering attacks, the research emphasized the need for advanced security measures, continuous training, strict laws, and technological advancements to effectively combat these attacks.

The importance of considering the human aspect in social engineering attacks is highlighted in [48], in which the authors propose a taxonomy of human factors that influence SE attacks. They argued that any analysis lacking a comprehensive exploration of these parameters would be considered deficient. To obtain a more comprehensive understanding, the authors outlined several key factors that should be included in this taxonomy, such as users' demographics, socio-emotional perspective, confidence, trust, perceptual abilities, privacy concerns, and education levels.

TABLE 2. Comparison of our study with existing studies in the literature.

Taxonomy Reference	Year of publication	Attacks taxonomy	Countermeasures taxonomy	Research challenges	Future directions
[18]	2014	✓	X	X	X
[43]	2014	✓	X	X	X
[44]	2015	✓	X	✓	X
[61]	2015	X	✓	✓	X
[45]	2017	✓	X	X	X
[46]	2019	✓	X	X	✓
[32]	2020	✓	X	X	✓
[62]	2020	X	✓	X	✓
[47]	2021	✓	X	✓	✓
[48]	2022	✓	X	X	✓
Our Taxonomy	-	✓	✓	✓	✓

It is worth noting that some of the reviewed studies focused on classifying a specific form of social engineering attack, such as phishing. For instance, in [49], the authors proposed a taxonomy of phishing attacks based on the different mechanisms that phishers use to access personal information, distinguishing between social engineering techniques (spoofed emails and fake websites) and technical subterfuge methods (cross-site scripting and session hijacking). In a similar vein, [50] proposed a comprehensive taxonomy for e-mail-based phishing attacks consisting of six phases categorized based on specific categorization criteria.

B. TAXONOMIES OF SE COUNTERMEASURES

While the reviewed articles provide valuable insights into the classification and categorization of social engineering attacks, it can be observed that comparatively less attention has been given to the development of taxonomies focusing specifically on social engineering countermeasures. The majority of studies addressing classifications of social engineering countermeasures have primarily focused on classifying solutions to counter specific attacks, with a particular emphasis on phishing attacks [51], [52], [53], [54], [55], [56], [57], [58], [59]. This is likely due to the fact that phishing attacks are among the most common and well-known forms of social engineering, and they constitute the biggest threat to both individuals and organizations [60].

It is essential to note that fewer studies have addressed the classification of defense mechanisms and countermeasures for preventing social engineering attacks in light of their wide range of attack types. For instance, in [61], the authors proposed a taxonomy for social engineering detection techniques, categorizing attacks into human-based and technology-based. They emphasized the importance of combining both approaches for effective detection and prevention. Human-based mitigation methods involve human intervention in detecting and preventing social engineering attacks. This includes policies, auditing, education, training, and awareness approaches. Technology-based mitigation methods rely on technological systems to detect and prevent social engineering attacks. This includes the use of sensors for physical identity verification, biometrics for verifying the identity of individuals, artificial intelligence for analyzing patterns and behaviors, and social honeypots for trapping social engineers.

In another study, [62], the authors presented a taxonomy for social engineering defense mechanisms based on five main target points: people, data, software and hardware (SW/HW), and networks. They outlined defense mechanisms for each target point to prevent social engineering attacks. For people, organizations should educate employees and hire IT personnel knowledgeable in social engineering and security expertise. Regarding data, organizations should conduct regular backups, establish clear security policies, and determine the bare minimum of information required. For software and hardware, employees must be educated on the management process, work communications, authentication policies, and bring-your-own-device (BYOD) policies. Regarding networks, employees need to be aware of different security policies based on the network type and be cautious when accessing networks remotely.

C. COMPARATIVE ANALYSIS

Comparing our study to the reviewed studies, it is evident, as shown in Table 2, that our research addresses some of the limitations found in the previous works. Our study presents comprehensive taxonomies that address both social engineering attacks themselves and their corresponding countermeasures, whereas the reviewed studies focus on either proposing a social engineering attack taxonomy or a taxonomy for countermeasures. The importance of providing taxonomies for both attacks and their countermeasures cannot be overlooked. A taxonomy that only addresses one aspect of the problem may lead to an incomplete comprehension of the SE landscape. However, by covering both SE attacks and countermeasures, we provide a more complete understanding of the SE landscape, which is crucial for developing effective defense strategies. Moreover, our study goes beyond the scope of previous research by highlighting research challenges and outlining future directions in evolving SE taxonomies. We propose other potential levels, dimensions, and aspects, such as the attacker's objectives, attack complexity, and targets, for researchers to explore. These additional levels

can serve as a foundation for developing more exhaustive taxonomies, fostering further research and innovation in SE attack prevention and mitigation.

V. THE PROPOSED TAXONOMY OF SE ATTACKS

The primary objective of this section is to investigate the research question (RQ1). In this study, the proposed taxonomy of social engineering (SE) attacks is a multi-layered framework designed to systematically categorize and understand the various methods, approaches, and tools employed by attackers to manipulate their targets, enabling researchers, practitioners, and organizations to analyze and respond to these threats more effectively. Each attack is assigned to its corresponding category based on the specific environment in which it occurs, the approach employed to manipulate the target, and the medium through which the attack is executed.

Table 3 lists all the attacks mentioned in the proposed taxonomy, along with their corresponding environments, approaches, mediums, and comprehensive justifications for their classifications. As shown in Fig. 4, this comprehensive taxonomy is organized into three levels:

A. ENVIRONMENT

The environment level distinguishes between in-person and remote attacks, highlighting the different contexts in which these attacks occur and emphasizing the physical presence or absence of the attacker.

- **In-person Attacks:** This category encompasses attacks that occur in physical proximity to the target, emphasizing the physical presence of the attacker. These attacks often involve face-to-face interactions and physical access to the target's environment.
- **Remote Attacks:** This category involves attacks that are executed from a distance, often using psychological triggers, and leveraging digital communication channels and tools. The absence of physical proximity is a key characteristic of remote attacks.

B. APPROACHES

This level encompasses the tactics, strategies, and psychological triggers employed by attackers to manipulate their victims. These approaches represent the underlying strategies and motivations behind social engineering attacks, each targeting different aspects of human psychology and behavior. The approaches are categorized into two main categories:

- **Physical-based:** This approach involves exploiting physical access or proximity to the target to conduct the social engineering attack.
- **Psychological triggers-based:**This approach involves exploiting various aspects of human psychology, such as curiosity, fear, greed, and trust, to manipulate individuals into taking actions that may compromise their security or divulge sensitive information.
  - **Curiosity-based:** This approach leverages the target's natural curiosity to entice them into taking actions that compromise their security, such as clicking on malicious links or downloading malware.
  - **Fear/Urgency-based:** This approach leverages the emotions of fear and urgency to prompt victims to take immediate action without critically evaluating the situation.
  - **Greed-based:** This approach exploits the target's desire for personal gain or advantage, often by offering something in exchange for sensitive information or unauthorized access to a secure system.
  - **Trust-based:** This approach involves exploiting the natural human tendency to trust others. Attackers use this approach to establish a sense of trust with their victims through various means, such as creating fabricated scenarios or impersonating trusted entities. Once trust is established, the attackers manipulate the victims into providing sensitive information or access.

C. MEDIUMS

This level encompasses the specific channels, tools, or means used to execute the attack. Understanding the mediums employed in SE attacks is crucial, as it allows organizations to identify potential points of entry and develop appropriate security measures tailored to each type of attack.

- **Physical Access:** This medium involves gaining physical access to restricted areas or resources, such as offices, data centers, or storage areas, to obtain sensitive information or conduct malicious activities. This is frequently accomplished by exploiting the absence of adequate access control measures through strategies such as tailgating.
- **Physical Interaction:** This medium involves direct and in-person interaction with the target, such as posing as an authority figure or expert to manipulate the victim into providing information or access to restricted areas. For instance, the attacker might pose as a technician from a trusted service provider (e.g., an internet company) and visit a corporate office under the guise of performing routine maintenance or upgrades (reverse social engineering attack, pretexting attack).
- **Physical Information Retrieval:** This method refers to the process of acquiring confidential data through physical means by physically accessing a company's trash or discarded materials and exploiting the oversight of organizations in properly disposing of confidential documents and materials. This strategy is commonly known as dumpster diving.
- **Observation-based:** This approach involves gathering sensitive information by directly observing the target's actions or behaviors without their knowledge. For example, an individual standing behind someone at an ATM and observing them enter their PIN to withdraw money is engaging in a shoulder-surfing attack.

TABLE 3. Rationale for SE attacks classification.

Attacks	Environment	Approaches	Mediums	Rationale for Classification
Tailgating	In-person	Physical-based	Physical access	This attack involves following someone into a restricted area without authorization, and it requires physical proximity.
Dumpster Diving	In-person	Physical-based	Physical information retrieval	This attack involves the attacker physically searching through a company's trash or discarded materials (e.g., hard drives, CDs) to obtain sensitive information that can be used for further attacks.
Shoulder Surfing	In-person	Physical-based	Observation-based	This attack involves physically and directly observing the victim's actions, such as typing a password or entering a PIN, to obtain sensitive information without their knowledge.
Watering Hole	Remote	Curiosity-based	Website-based	This attack involves infecting a website frequently visited by the target group. It can be executed remotely through a compromised website.
Phishing	Remote	Curiosity-based	Email-based/ Websites-based/ Software-based	This attack involves sending fraudulent emails that appear to be from a legitimate source, typically remotely through email, fake websites, software, or messaging apps.
Spear Phishing	Remote	Curiosity-based	Email-based	This attack is similar to phishing, but it targets specific individuals or organizations, and it can be executed remotely through email or messaging apps.
Whaling	Remote	Curiosity-based	Email-based	This attack involves targeting high-level executives or decision-makers within an organization with fraudulent emails.
Scareware	Remote	Fear/Urgency-based	Software-based	This attack involves using fake security alerts or warnings to trick victims into downloading and installing malicious software or paying for fake security products.
Smishing	Remote	Fear/Urgency-based	SMS-based	This attack involves using fraudulent text messaging to trick individuals, and it can be executed remotely through messaging apps.
Vishing	Remote	Fear/Urgency-based	VoIP-based	This attack involves using voice communication to impersonate a legitimate source, and it can be executed remotely through phone.
Quid Pro Quo	Remote	Greed-based	VoIP-based	This attack involves offering something (e.g., a service or benefit) in exchange for sensitive information or access, typically remotely over voice communication channels.
Baiting	In-person/ Remote	Curiosity-based/Greed-based	Physical access/ Removable Media-based	This attack involves leaving malware-infected devices (e.g., USB drives, CDs) in strategic locations, enticing victims to insert the media into their computers, and then gaining remote control.
Reverse Social Engineering	In-person/ Remote	Physical-based/Trust-based	Physical interaction/ VoIP-based	This attack involves the attacker posing as an authority figure or expert to manipulate the victim into providing information or access.
Pretexting	In-person/ Remote	Physical-based/Trust-based	Physical interaction/VoIP-based	This attack involves creating a fabricated scenario or pretext to establish trust with the victim. It can typically be executed in-person or remotely through voice communication channels.

- **Website-based:** This medium involves exploiting vulnerabilities in websites to deliver malware or using deceptive websites to trick visitors into revealing sensitive information or downloading malware. Attackers may infect legitimate websites frequented by their targets with malware (watering hole attack) or create fake websites that mimic trusted platforms, such as online banking portals or social media sites (phishing attack).
- **Email-based:** This medium involves the use of fraudulent or deceptive emails to trick recipients into clicking on malicious links, downloading malware, or divulging sensitive information. For instance, an email claiming to be from a legitimate and well-known bank might ask the recipient to urgently update their account information by clicking on a link, which leads to a fraudulent website designed to steal their login credentials. Phishing, spear-phishing, and whaling are common forms of email-based attacks.
- **Software-based:** This medium involves using fake security alerts or warnings to trick victims into downloading and installing malicious software or paying for false security products. Attackers may utilize deceptive pop-up windows to mislead users into installing malicious software under the guise of system updates or essential security utilities (scareware attack). Additionally, phishers may use malicious software, such as keyloggers or spyware, to gather sensitive information entered by users on their devices without their knowledge (phishing attack).
- **SMS-based:** This medium involves leveraging text messages to deceive victims into taking actions that

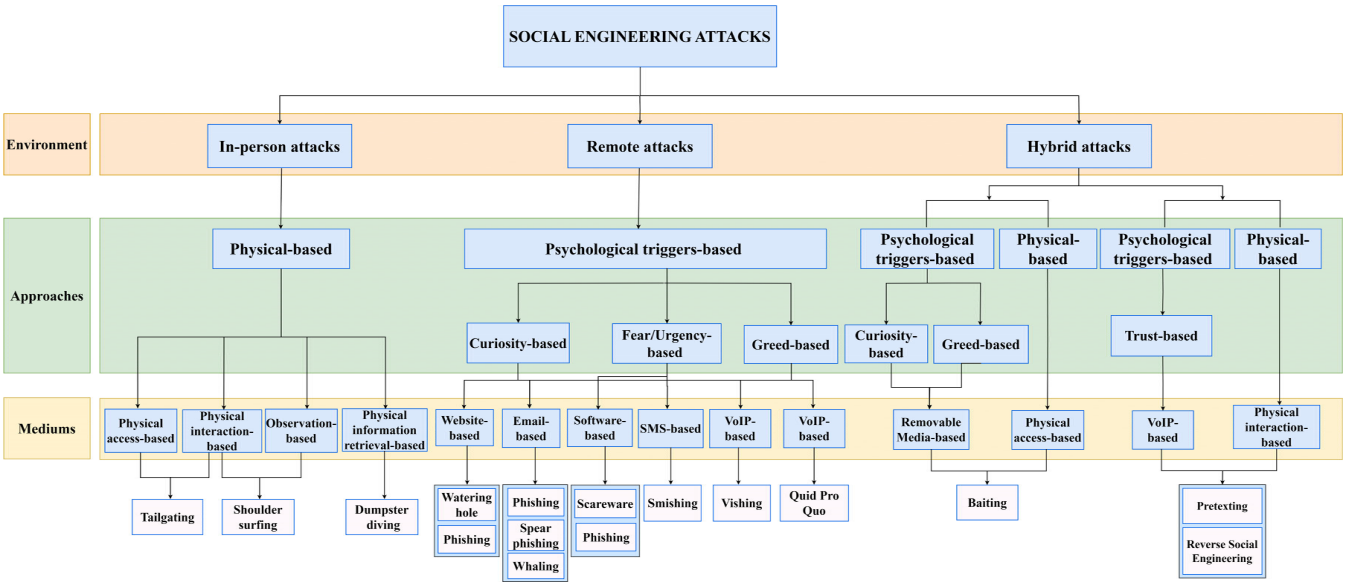


FIGURE 4. The proposed taxonomy of SE attacks.

compromise their security, such as clicking on malicious links or revealing sensitive information. For example, the user may receive a text message claiming to be from their bank, stating that their account has been compromised and urging them to click on a link to verify their details. This link leads to a fake website designed to steal their login credentials and personal information (smishing).

- **VoIP-based:** This medium involves using voice communication to impersonate a legitimate source and trick individuals into revealing sensitive information or performing actions that compromise their security. For instance, the attacker may use a VoIP service to make phone calls, posing as a legitimate entity such as a bank or government agency, to trick their targets into revealing personal information like credit card numbers or passwords (vishing attack). Another example involves leveraging VoIP to fabricate a false scenario or pretext, such as impersonating a co-worker or IT support, to manipulate victims into providing sensitive information or performing actions that compromise security (pretexting attack). Quid pro quo is also a VoIP-based attack where the hacker offers assistance in exchange for the opportunity to compromise the company's security. For example, an attacker might also call employees within a company, pretending to be from the IT department. The hacker proposes assisting the employees by remotely accessing their computers to provide a ''software upgrade'' or ''security patch''.
- **Removable Media-based:** This medium involves the use of physical media, such as USB drives or CDs, to distribute malware or deceive individuals into compromising their systems by inserting the media and allowing remote control. An example of this is a baiting attack, in which the attacker leaves an infected USB flash drive in a workplace in hopes that an employee will find it and unknowingly plug it into their computer, giving the hacker access and control. This kind of attack preys on the employee's curiosity and desire for privileged information, making them more likely to fall for the bait.

It is worth noting that these classifications are not necessarily mutually exclusive, and some social engineering attacks may fall into multiple categories depending on the specific techniques used. Some attacks can be considered hybrids due to their combination of in-person and remote elements. However, it's important to note that the classification of an attack as a hybrid can vary depending on the specific tactics and techniques used by the attacker. For instance, baiting can be classified as a hybrid attack due to its combination of in-person placement of physical bait (e.g., infected USB drives) and the subsequent remote action when the bait is interacted with on a computer. The pretexting attack can also be considered a hybrid attack. While it typically involves remote communication (e.g., phone calls), it can also involve in-person interactions where the attacker physically presents themselves to the target to build credibility or manipulate the situation. Similarly, reverse social engineering can occur both in-person and remotely. In an in-person scenario, the attacker may physically interact with the victim to manipulate them into divulging sensitive information or performing actions that compromise security. In a remote scenario, the attacker may use various communication channels, such as phone calls, to achieve the same goal.

VI. THE PROPOSED TAXONOMY OF SE COUNTERMEASURES

In this section, we aim to address the research question (RQ3) by proposing a comprehensive taxonomy of social engineering countermeasures to combat the persistent and evolving threat presented by social engineering attacks. As illustrated in Fig. 5, the taxonomy consists of four essential categories:

- **Awareness and Training:** This category focuses on educating individuals about social engineering attacks and how to recognize and respond to them.
- **Technical Controls:** This category involves implementing technological measures to prevent and detect social engineering attacks.
- **Policies, Procedures, and Governance:** This category focuses on establishing policies, procedures, and governance frameworks to mitigate social engineering risks.
- **Incident Response and Reporting** This category deals with the processes and protocols for responding to social engineering incidents.

By organizing and categorizing these countermeasures, organizations can obtain a comprehensive understanding of the necessary elements for a robust defense against social engineering attacks. This taxonomy provides organizations with a valuable framework for identifying and implementing effective strategies that encompass the prevention, detection, response, and mitigation of social engineering incidents.

A. AWARENESS AND TRAINING-BASED MECHANISMS

- **Social engineering and phishing Awareness Training (1a):** This involves educating employees about the various social engineering techniques and keeping them updated on the latest tactics and defense mechanisms. It also includes training sessions supplemented with simulated attacks, providing a practical scenario for employees to test their awareness and preparedness, and practical guidance on recognizing and avoiding phishing attempts, including suspicious emails, links, and attachments [64], [65], [66], [67].
- **Password Security Training (1b):** This involves educating employees on best practices for creating strong passwords. It also includes training on the risks associated with password reuse and sharing [68], [69].
- **Safe Online Behavior Education (1c):** This involves educating employees about safe online practices, such as avoiding downloading unknown attachments, clicking on suspicious links, and being cautious when sharing personal or company information online [70].

B. TECHNICAL-BASED MECHANISMS

- **Email, SMS Filters, and Anti-Spam Solutions (2a):** These tools utilize filtering mechanisms to identify and block phishing emails and spam messages that may contain malicious links or attachments before they reach the recipients' inboxes [71], [72].
- **Two-Factor Authentication (2FA) Implementation (2b):** Two-factor authentication (2FA) is a security process that requires users to provide two forms of identification to access an account, system, or application. It adds an extra layer of security to the authentication process by requiring users to provide something they know (such as a password) and something they have (such as a verification code sent to a mobile device) [73], [74].
- **Firewall and Intrusion Detection/Prevention Systems (2c):** Deployed to monitor and block unauthorized access attempts and identify potential intrusion or malicious activities [75], [76].
- **Security Information and Event Management (SIEM) Solutions (2d):** SIEM solutions collect and analyze security events and logs from various sources to detect and respond to suspicious activities [77].
- **Endpoint Protection and Anti-Malware Solutions (2e):** These solutions protect individual devices (endpoints) from malware and other malicious software that can be used in social engineering attacks [76], [78].
- **Caller ID and Call Filtering Solutions (2f):** These solutions help identify and block fraudulent or spoofed calls, protecting against voice-based social engineering attacks [79], [80], [81].
- **Browser Security Features and Extensions Deployment (2g):** Enhancing web browser security with features and extensions that detect and block malicious websites, phishing attempts, and other online threats [56], [84].
- **AI-based countermeasures (2h):**As a powerful tool, artificial intelligence (AI) can play a vital role in detecting and preventing social engineering attacks. It can analyze communication patterns, identify anomalies, and simulate realistic scenarios for engaging training. Furthermore, AI can thoroughly examine messages and links, flag potential threats, and analyze data for breach indicators. In the event of an attack, AI streamlines incident response by automating tasks and learning from incidents to enhance security measures [82], [83].

C. POLICY AND PROCEDURE-BASED MECHANISMS

- **Access Control Policies and User Permissions Management (3a):** These policies define who has access to what resources and how user privileges are managed, reducing the risk of unauthorized access and ensuring access to systems, applications, and data based on job roles and responsibilities [85], [86].
- **Password Management Policies (3b):** These policies establish guidelines and best practices for creating, securely storing, and changing passwords, promoting good password hygiene to ensure secure authentication, and reducing the risk of password-related social engineering attacks [87], [88].
- **Acceptable Use Policies (3c):** These policies outline acceptable behavior and actions when using

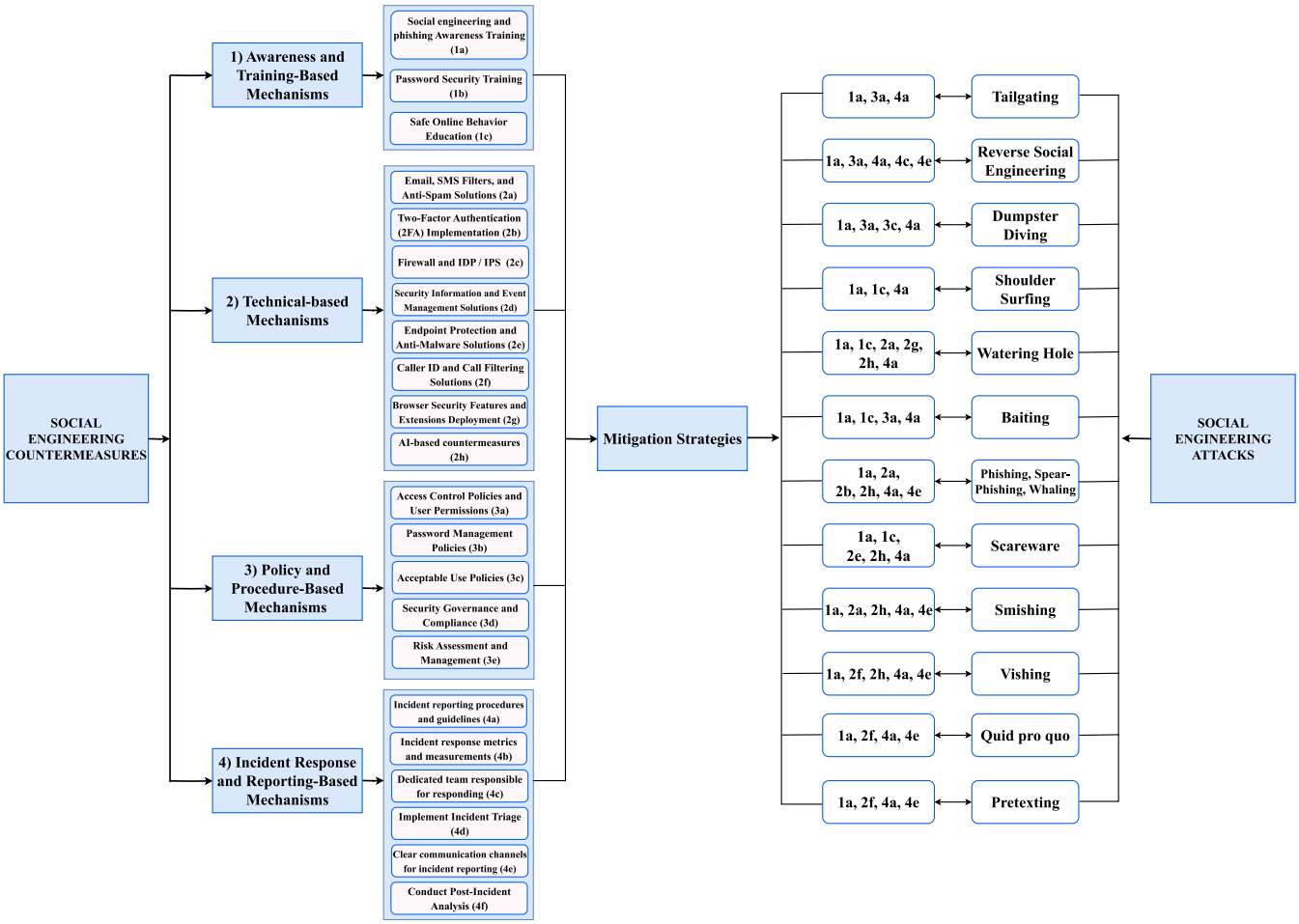


FIGURE 5. Taxonomy and optimal mitigation strategies for SE countermeasures.

organizational resources, systems, and networks, emphasizing security responsibilities and restrictions [89].

- **Security Governance and Compliance (3d):** This involves establishing a framework for managing security risks, implementing controls, ensuring compliance with relevant regulations and standards, and providing oversight for social engineering countermeasures [90].
- **Risk Assessment and Management (3e):** This process involves identifying and assessing vulnerabilities and potential risks, prioritizing them, and implementing appropriate controls and mitigation strategies [91].

D. INCIDENT RESPONSE AND REPORTING-BASED MECHANISMS

- **Incident reporting procedures and guidelines (4a):** These procedures outline the steps and instructions for reporting a suspected or confirmed social engineering incident, ensuring timely reporting, and including the necessary information and channels to notify the appropriate teams. [92].
- **Incident response metrics and measurements (4b):** Establishes metrics and key performance indicators (KPIs) to assess the effectiveness and efficiency of incident response efforts, and identify areas for improvement [92].
- **Establishing a dedicated team responsible for responding (4c):** This involves forming a specialized team with the necessary skills and expertise to handle social engineering incidents promptly and effectively [93].
- **Implement Incident Triage (4d):** Develops a structured process for assessing and prioritizing incidents based on severity, impact, and urgency to prioritize response efforts and allocate appropriate resources [94].
- **Clear communication channels and protocols for incident reporting (4e):** Ensures that employees have accessible and well-defined communication channels to report incidents securely and efficiently [93].
- **Conduct Post-Incident Analysis (4f):** This involves reviewing and analyzing social engineering incidents after they occur to identify lessons learned and root causes, evaluate response effectiveness, and implement improvements to prevent similar incidents in the future [95].

TABLE 4. SE attack vectors, mitigation strategies, and rationale.

Attack	Attack Vector	Mitigation strategies	Rationale for strategies
Tailgating	Physical access-based	1a, 3a, 4a	Awareness training, access control policies, and incident reporting can help prevent unauthorized access.
Dumpster Diving	Physical information retrieval-based	1a, 3a, 3c, 4a	Awareness training, access control policies, acceptable use policies, and incident reporting can help protect sensitive information.
Shoulder Surfing	Observation-based	1a, 1c, 4a	Awareness training, safe online behavior education, and incident reporting can help prevent unauthorized observation.
Watering Hole	Website-based	1a, 1c, 2a, 2g, 2h, 4a	Awareness training, safe online behavior education, email filters, browser security features, artificial intelligence, and incident reporting can help protect against malicious websites.
Baiting	Removable Media-based	1a, 1c, 3a, 4a	Awareness training, safe online behavior education, access control policies, and incident reporting can help prevent unauthorized access.
Phishing, Spear Phishing, Whaling	Email-based/ Websites-based/ Software-based	1a, 2a, 2b, 2h, 4a, 4e	Awareness training, email filters, two-factor authentication, AI-based detection, incident reporting, and clear communication channels can help protect against email-based attacks.
Scareware	Software-based	1a, 1c, 2e, 2h, 4a	Awareness training, safe online behavior education, endpoint protection, AI-based detection ,and incident reporting can help protect against malicious software.
Smishing	SMS-based	1a, 2a, 2h, 4a, 4e	Awareness training, SMS filters, I-based detection, incident reporting, and clear communication channels can help protect against SMS-based attacks.
Vishing	VoIP-based	1a, 2f, 2h, 4a, 4e	Awareness training, caller ID and call filtering solutions, AI-based detection, incident reporting, and clear communication channels can help protect against VoIP-based attacks.
Quid Pro Quo	VoIP-based	1a, 2f, 4a, 4e	Awareness training, caller ID and call filtering solutions, incident reporting, and clear communication channels can help protect against VoIP-based attacks.
Reverse Social Engineering	Physical interaction-based	1a, 3a, 4a, 4c, 4e	Awareness training, access control policies, caller ID and call filtering solutions, AI-based detection, incident response team, and clear communication channels can help prevent manipulation.
Pretexting	VoIP-based	1a, 2f, 4a, 4e	Awareness training, caller ID and call filtering solutions, incident reporting, and clear communication channels can help protect against VoIP-based attacks.

Fig. 5 presents a well-organized taxonomy of all attack forms discussed in this paper, along with the optimal mitigation strategies, while Table 4 provides justifications for implementing these specific countermeasures.

VII. GRAND RESEARCH CHALLENGES AND FUTURE RESEARCH DIRECTIONS

As technological progress continues, malicious actors continually adapt their tactics to exploit the vulnerabilities of individuals. This section aims to address the research question (RQ3) by highlighting the grand challenges in social engineering research and exploring future research directions.

A. GRAND RESEARCH CHALLENGES

- **Challenge 1 - Deep understanding of human behavior:** One of the primary challenges in social engineering research is gaining a deep understanding of human behavior and decision-making processes. Human beings exhibit various motivations, cognitive biases, and emotional reactions. Researchers need to delve deeper into the complexities of human psychology and analyze in-depth cultural factors that influence human behavior in order to uncover the underlying mechanisms that make individuals susceptible to social engineering attacks [96], [97].
- **Challenge 2 - Real-Time behavioral analysis:** Real-time behavioral analysis is crucial for detecting and mitigating social engineering attacks. Future research should focus on developing advanced techniques and algorithms capable of analyzing and interpreting behavioral data in real-time, identifying patterns and indicators associated with suspicious activity. This includes leveraging the power of artificial intelligence and data analytics to enhance the effectiveness and efficiency of real-time behavioral analysis systems [98].
- **Challenge 3 - Evaluating the effectiveness of countermeasures:** Developing countermeasures against social engineering attacks is an ongoing challenge, and measuring the effectiveness of these countermeasures is a significant challenge. Researchers need to evaluate the effectiveness of existing solutions and identify areas for enhancement. This involves conducting rigorous testing, analyzing real-world case studies, evaluating both modern and traditional training and awareness programs, technological solutions, and organizational policies, and collaborating with industry professionals and government agencies to ensure that countermeasures are practical and efficient in mitigating the risks posed by social engineering attacks [99], [100].
- **Challenge 4 - Bridging the gap between research and practice:** Bridging the gap between research and practice is a significant challenge in the field of social engineering. Although research provides valuable insights into the tactics and vulnerabilities associated with social engineering attacks, it is crucial to translate these findings into practical strategies that can be effectively implemented by organizations and individuals.

This requires collaboration and knowledge exchange between researchers, practitioners, and industry experts to ensure that research findings are relevant, actionable, and applicable in real-world contexts [101].

- **Challenge 5 - Authoritative and real-world data collection:** Collecting authoritative and real-world data for social engineering research can be challenging due to legal, ethical, and privacy considerations. However, obtaining such data is essential for conducting credible research and effective studies [44].
- **Challenge 6 - Addressing legal and ethical implications:** Social engineering research raises legal and ethical concerns due to its potential for misuse, particularly when it involves manipulating human behavior for experimental purposes. Researchers must address these challenges to strike a balance between research objectives and ethical responsibilities. This requires adhering to ethical guidelines, obtaining informed consent, and ensuring the privacy and safety of participants involved in social engineering research [102], [103].
- **Challenge 7 - Predicting susceptibility to social engineering attacks in real-time:** Predicting susceptibility to social engineering attacks in real-time is a challenging yet valuable endeavor in the field of cybersecurity. This requires a multidisciplinary approach that leverages human psychology, behavior analysis, sophisticated technologies, machine learning, real-time data processing, and ongoing monitoring. A central challenge is identifying automatically measurable features that correlate with susceptibility to social engineering attacks. These features should provide reliable indicators of vulnerability to manipulation [44].
- **Challenge 8 - Deepfake social engineering attacks:** The emergence of deepfake technology presents new social engineering challenges. Deepfake social engineering attacks involve the use of altered audio or video content to deceive individuals and manipulate their behavior. Future research should focus on comprehending the impact of deepfake social engineering attacks, developing detection and prevention techniques, and investigating the psychological factors that make individuals susceptible to such attacks [82].

B. FUTURE DIRECTIONS

In light of the dynamic and evolving nature of social engineering attacks, this taxonomy should be viewed as a starting point, with future research needed to refine and expand it by including other potential levels, dimensions, and aspects, such as the attacker's objectives, attack complexity, and targets. Understanding the attacker's objectives can provide insights into the motivations behind different social engineering attacks. Analyzing attack complexity can help in understanding the sophistication level of social engineering attacks, which can range from basic to advanced. Identifying the targets can assist in understanding who is most at risk, whether they are individuals, companies, or organizations. Moreover, future research should focus on real-world examples and conduct a thorough analysis of all social engineering attack scenarios. Qualitative studies, such as victim interviews, are also recommended to gain a deeper understanding of the techniques used by attackers. In addition, exploring gamification and simulation in the context of combating social engineering attacks is a promising avenue for future research. These techniques can create a realistic and engaging environment, improve the effectiveness of training programs, and simulate real-world social engineering scenarios.

VIII. CONCLUSION

In conclusion, this research paper provides comprehensive taxonomies of social engineering attacks and countermeasures, categorizing these attacks into three distinct levels: environment, approaches, and mediums. The corresponding taxonomy for social engineering countermeasures is designed to offer a range of defenses and mitigation strategies that can be employed based on the specific nature of the attack. The practical implications of these taxonomies are crucial for organizations seeking to improve their mitigation strategies, safeguard their valuable assets, and maintain stakeholder confidence. The proposed taxonomies serve as a valuable tool for researchers, practitioners, and organizations to understand the landscape of social engineering threats and countermeasures. Firstly, they provide a structured framework for analyzing and comparing different types of social engineering attacks and countermeasures. This allows organizations to assess their current security measures and identify any gaps or vulnerabilities that need to be addressed. Secondly, the taxonomies facilitate the development of adequate training programs. This targeted training equips employees with the knowledge and skills necessary to recognize and respond effectively to social engineering attempts. Finally, the taxonomies enable organizations to review, update, or create effective security policies.

CONFLICT OF INTEREST STATEMENT

The authors declare that there are no conflicts of interest regarding the publication of this paper.

REFERENCES

[1] H. de Bruijn and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Government Inf. Quart.*, vol. 34, no. 1, pp. 1–7, Jan. 2017, doi: 10.1016/j.giq.2017.02.007.

[2] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Comput. Secur.*, vol. 73, pp. 102–113, Mar. 2018, doi: 10.1016/j.cose.2017.10.008.

[3] P. Zambrano, J. Torres, L. Tello-Oquendo, Á. Yánez, and L. Velásquez, "On the modeling of cyber-attacks associated with social engineering: A parental control prototype," *J. Inf. Secur. Appl.*, vol. 75, Jun. 2023, Art. no. 103501, doi: 10.1016/j.jisa.2023.103501.

[4] B. Schneier, *Secrets and Lies : Digital Security in a Networked World. Indianapolis*. Hoboken, NJ, USA: Wiley, 2015.

[5] G. Öçütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Comput. Secur.*, vol. 56, pp. 83–93, Feb. 2016, doi: 10.1016/j.cose.2015.10.002.

[6] Z. Yan, T. Robertson, R. Yan, S. Y. Park, S. Bordoff, Q. Chen, and E. Sprissler, "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?" *Comput. Hum. Behav.*, vol. 84, pp. 375–382, Jul. 2018, doi: 10.1016/j.chb.2018.02.019.

[7] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, Mar. 2018, doi: 10.1016/j.cose.2017.11.015.

[8] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, Oct. 2020, doi: 10.1007/s11235-020-00733-2.

[9] M. Bhattacharya, S. Roy, K. Mistry, H. P. H. Shum, and S. Chattopadhyay, "A privacy-preserving efficient location-sharing scheme for mobile online social network applications," *IEEE Access*, vol. 8, pp. 221330–221351, 2020, doi: 10.1109/ACCESS.2020.3043621.

[10] S. Venkatesha, K. R. Reddy, and B. R. Chandavarkar, "Social engineering attacks during the COVID-19 pandemic," *Social Netw. Comput. Sci.*, vol. 2, no. 2, pp. 1–18, Feb. 2021, doi: 10.1007/s42979-020-00443-1.

[11] Verizon. (2023). *Data Breach Investigations Report*. Accessed: Jun. 25, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[12] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021, doi: 10.1109/ACCESS.2021.3051633. https://doi.org/10.1109/access.2021.3051633

[13] M. Hijji and G. Alam, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions," *IEEE Access*, vol. 9, pp. 7152–7169, 2021, doi: 10.1109/ACCESS.2020.3048839. https://doi.org/10.1109/access.2020.3048839

[14] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, vol. 59, pp. 186–209, Jun. 2016, doi: 10.1016/j.cose.2016.03.004.

[15] W. Fan, K. Lwakatare, and R. Rong, "Social engineering: I-E based model of human weakness for attack and defense investigations," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 1, pp. 1–11, Jan. 2017, doi: 10.5815/ijcnis.2017.01.01.

[16] K. F. Steinmetz, A. Pimentel, and W. R. Goe, "Performing social engineering: A qualitative study of information security deceptions," *Comput. Hum. Behav.*, vol. 124, Nov. 2021, Art. no. 106930, doi: 10.1016/j.chb.2021.106930.

[17] C. C. Campbell, "Solutions for counteracting human deception in social engineering attacks," *Inf. Technol. People*, vol. 32, no. 5, pp. 1130–1152, Oct. 2019, doi: 10.1108/itp-12-2017-0422.

[18] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[19] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019, doi: 10.3390/fi11040089.

[20] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3, p. 73, Mar. 2019, doi: 10.3390/fi11030073.

[21] H. Aldawood and G. Skinner, "Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions," *IEEE Access*, vol. 8, pp. 67321–67329, 2020, doi: 10.1109/ACCESS.2020.2983280. https://doi.org/10.1109/access.2020.2983280

[22] Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, 2020, doi: 10.1109/ACCESS.2020.2992807. https://doi.org/10.1109/access.2020.2992807

[23] A. Yasin, R. Fatima, L. Liu, A. Yasin, and J. Wang, "Contemplating social engineering studies and attack scenarios: A review study," *Secur. Privacy*, vol. 2, no. 4, pp. 1–17, Jun. 2019.

[24] C. Hadnagy, *Social Engineering : The Art of Human Hacking*. Hoboken, NJ, USA: Wiley, 2011.

[25] N. Yathiraju, G. Jakka, S. K. Parisa, and O. Oni, *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security*. Hershey, PA, USA: IGI Global, 2022, pp. 110–132.

[26] S. Lohani. (2019). *Social Engineering: Hacking Into Humans*. Accessed: Feb. 05, 2019. [Online]. Available: https://ssrn.com/abstract=3329391

[27] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," *Inf. Secur. South Afr.*, pp. 1–9, Aug. 2014, doi: 10.1109/issa.2014.6950510.

[28] P. L. Gallegos-Segovia, J. F. Bravo-Torres, V. M. Larios-Rosillo, P. E. Vintimilla-Tapia, I. F. Yuquilima-Albarado, and J. D. Jara-Saltos, "Social engineering as an attack vector for ransomware," in *Proc. Conf. Elect., Electron. Eng.*, Oct. 2017, pp. 1–6.

[29] K. Chetioui, B. Bah, A. O. Alami, and A. Bahnasse, "Overview of social engineering attacks on social networks," *Proc. Comput. Sci.*, vol. 198, pp. 656–661, Jan. 2022.

[30] M. Bhattacharya, S. Roy, S. Chattopadhyay, A. K. Das, and S. S. Jamal, "ASPA-MOSN: An efficient user authentication scheme for phishing attack detection in mobile online social networks," *IEEE Syst. J.*, vol. 17, no. 1, pp. 234–245, Mar. 2023, doi: 10.1109/JSYST.2022.3168234.

[31] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Social engineering attacks on the knowledge worker," in *Proc. 6th Int. Conf. Secur. Inf. Netw.*, Nov. 2013, pp. 1–17, doi: 10.1145/2523514.2523596.

[32] H. Aldawood and G. Skinner, "An advanced taxonomy for social engineering attacks," *Int. J. Comput. Appl.*, vol. 177, no. 30, pp. 1–11, Jan. 2020, doi: 10.5120/ijca2020919744.

[33] F. Breda, H. Barbosa, and T. Morais, "Social engineering and cyber security," in *Proc. INTED*, Mar. 2017, pp. 4204–4211, doi: 10.21125/inted.2017.1008.

[34] N. Y. Conteh and P. J. Schmick, "Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks," in *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*. 2021, pp. 19–31.

[35] J. S. Mollri, K. Petersen, and E. Mendes, "Survey guidelines in software engineering," in *Proc. ACM/IEEE Int. Symp. Empirical Softw. Eng. Meas.*, Sep. 2016, pp. 1–6, doi: 10.1145/2961111.2962619.

[36] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, May 2014, pp. 1–18, doi: 10.1145/2601248.2601268.

[37] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe, "A master attack methodology for an AI-based automated attack planner for smart cities," *IEEE Access*, vol. 6, pp. 48360–48373, 2018, doi: 10.1109/ACCESS.2018.2867556. https://doi.org/10.1109/access.2018.2867556

[38] O. Medelyan, I. H. Witten, A. Divoli, and J. Broekstra, "Automatic construction of lexicons, taxonomies, ontologies, and other knowledge structures," *WIREs Data Mining Knowl. Discovery*, vol. 3, no. 4, pp. 257–279, Jul. 2013, doi: 10.1002/widm.1097.

[39] Y. Sadqi and Y. Maleh, "A systematic review and taxonomy of web applications threats," *Inf. Secur. J., A Global Perspective*, vol. 31, no. 1, pp. 1–27, Dec. 2020, doi: 10.1080/19393555.2020.1853855.

[40] C. F. M. Foozy, R. Ahmad, M. F. Abdollah, R. Yusof, and M. Z. Masud, "Generic taxonomy of social engineering attack and defence mechanism for handheld computer study," in *Proc. Malaysian Tech. Universities Int. Conf. Eng. Technol.*, 2011, pp. 1–6.

[41] K. Ivaturia and L. Janczewski, "A taxonomy for social engineering attacks," in *Proc. Conf. IRM*, 2011, pp. 324–334.

[42] P. S. Maan and M. Sharma, "Social engineering: A partial technical attack," *Int. J. Comput. Sci. Issues*, vol. 9, no. 2, pp. 557–559, 2012.

[43] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," in *Proc. IEEE Secur. Privacy Workshops*, May 2014, pp. 236–250.

[44] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Comput. Surveys*, vol. 48, no. 3, pp. 1–39, Dec. 2015, doi: 10.1145/2835375.

[45] A. Koyun and E. A. Janabi, "Social engineering attacks," *J. Multidisciplinary Eng. Sci. Technol.*, vol. 4, no. 6, pp. 7533–7538, 2017.

[46] H. Aldawood and G. Skinner, "A taxonomy for social engineering attacks via personal devices," *Int. J. Comput. Appl.*, vol. 178, no. 50, pp. 19–26, Sep. 2019, doi: 10.5120/ijca2019919411.

[47] P. Tulkarm, "A survey of social engineering attacks: Detection and prevention tools," *J. Theor. Appl. Inf. Technol.*, vol. 99, no. 18, pp. 1–12, 2021.

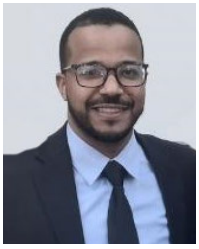
[48] A. Maraj and W. Butler, "Taxonomy of social engineering attacks: A survey of trends and future directions," in *Proc. Int. Conf. Cyber Warfare Secur.*, Mar. 2022, vol. 17, no. 1, pp. 185–193.

[49] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: Taxonomy of methods, current issues and future directions," *Telecommun Syst*, vol. 67, pp. 247–267, Feb. 2018.
[50] J. Rastenis, S. Ramanauskaitė, J. Janulevič ius, A. Čenys, A. Slotkienė, and K. Pakrijauskas, "E-mail-based phishing attack taxonomy," *Appl. Sci.*, vol. 10, no. 7, p. 2363, Mar. 2020, doi: 10.3390/app10072363.
[51] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, Dec. 2017, doi: 10.1007/s00521-016-2275-y.
[52] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Comput. Secur.*, vol. 68, pp. 160–196, Jul. 2017, doi: 10.1016/j.cose.2017.04.006.
[53] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Comput. Secur.*, vol. 73, pp. 519–544, Mar. 2018, doi: 10.1016/j.cose.2017.12.006.
[54] A. K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity based approaches," *Secur. Commun. Netw.*, vol. 2017, pp. 1–20, May 2017.
[55] M. Vijayalakshmi, S. M. Shalinie, M. H. Yang, and R. M. U., "Web phishing detection techniques: A survey on the state-of-the-art, taxonomy and future directions," *IET Netw.*, vol. 9, no. 5, pp. 235–246, Sep. 2020, doi: 10.1049/iet-net.2020.0078.
[56] S. Chanti and T. Chithralekha, "Classification of anti-phishing solutions," *Social Netw. Comput. Sci.*, vol. 1, no. 1, pp. 1–23, Jul. 2019, doi: 10.1007/s42979-019-0011-2.
[57] R. Zaimi, M. Hafidi, and M. Lamia, "Survey paper: Taxonomy of website anti-phishing solutions," in *Proc. 7th Int. Conf. Social Netw. Anal., Manage. Secur. (SNAMS)*, Dec. 2020, pp. 1–8, doi: 10.1109/SNAMS52053.2020.9336559.
[58] A. A. Alhashmi, A. Darem, and J. H. Abawajy, "Taxonomy of cybersecurity awareness delivery methods: A countermeasure for phishing threats," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 10, pp. 1–17, 2021, doi: 10.14569/ijacsa.2021.0121004.
[59] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep learning for phishing detection: Taxonomy, current challenges and future directions," *IEEE Access*, vol. 10, pp. 36429–36463, 2022, doi: 10.1109/ACCESS.2022.3151903. https://doi.org/10.1109/access.2022.3151903
[60] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *Int. J. Hum.-Comput. Stud.*, vol. 82, pp. 69–82, Oct. 2015, doi: 10.1016/j.ijhcs.2015.05.005.
[61] A. U. Zulkurnain, A. K. B. K. Hamidy, A. B. Husain, and H. Chizari, "Social engineering attack mitigation," *Int. J. Math. Comput. Sci.*, vol. 1, no. 4, pp. 188–198, 2015.
[62] D. N. Alharthi and A. C. Regan, "Social engineering defense mechanisms: A taxonomy and a survey of employees' awareness level," in *Intelligent Computing* (Advances in Intelligent Systems and Computing), vol. 1228. London, U.K. Jul. 2020, pp. 521–541.
[63] A. H. Washo, "An interdisciplinary view of social engineering: A call to action for research," *Comput. Hum. Behav. Rep.*, vol. 4, Aug. 2021, Art. no. 100126, doi: 10.1016/j.chbr.2021.100126.
[64] P. Schaab, K. Beckers, and S. Pape, "Social engineering defence mechanisms and counteracting training strategies," *Inf. Comput. Secur.*, vol. 25, no. 2, pp. 206–222, Jun. 2017, doi: 10.1108/ics-04-2017-0022.
[65] D. Airehrour, N. V. Nair, and S. Madanian, "Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model," *Information*, vol. 9, no. 5, p. 110, May 2018, doi: 10.3390/info9050110.
[66] I. Vayansky and S. Kumar, "Phishing—Challenges and solutions," *Comput. Fraud Secur.*, vol. 2018, no. 1, pp. 15–20, Jan. 2018.
[67] E. J. Williams, J. Hinds, and A. N. Joinson, "Exploring susceptibility to phishing in the workplace," *Int. J. Hum.-Comput. Stud.*, vol. 120, pp. 1–13, Dec. 2018, doi: 10.1016/j.ijhcs.2018.06.004.
[68] J. Saleem and M. Hammoudeh, "Defense methods against social engineering attacks," *Comput. Netw. Secur. Essentials*, pp. 603–618, Aug. 2017.
[69] M. Yıldırım and I. Mackie, "Encouraging users to improve password security and memorability," *Int. J. Inf. Secur.*, vol. 18, no. 6, pp. 741–759, Apr. 2019, doi: 10.1007/s10207-019-00429-y.
[70] R. W. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," *IEEE Secur. Privacy*, vol. 15, no. 5, pp. 55–64, May 2017, doi: 10.1109/MSP.2017.3681050.
[71] S. Mishra and D. Soni, "Smishing detector: A security model to detect smishing through SMS content analysis and URL behavior analysis," *Future Gener. Comput. Syst.*, vol. 108, pp. 803–815, Jul. 2020, doi: 10.1016/j.future.2020.03.021.
[72] A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti, and M. Alazab, "A comprehensive survey for intelligent spam email detection," *IEEE Access*, vol. 7, pp. 168261–168295, 2019, doi: 10.1109/ACCESS.2019.2954791. https://doi.org/10.1109/access.2019.2954791
[73] J. Gualdoni, A. Kurtz, I. Myzyri, M. Wheeler, and S. Rizvi, "Secure online transaction algorithm: Securing online transaction using two-factor authentication," *Proc. Comput. Sci.*, vol. 114, pp. 93–99, May 2017, doi: 10.1016/j.procs.2017.09.016.
[74] A. Kumar, M. Chaudhary, and N. Kumar, "Social engineering threats and awareness: A survey," *Eur. J. Adv. Eng. Technol.*, vol. 2, no. 11, pp. 15–19, 2015.
[75] T. Chin, K. Xiong, and C. Hu, "Phishlimiter: A phishing detection and mitigation approach using software-defined networking," *IEEE Access*, vol. 6, pp. 42516–42531, 2018, doi: 10.1109/ACCESS.2018.2837889. https://doi.org/10.1109/ACCESS.2018.2837889
[76] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, "Phishing attacks and defenses," *Int. J. Secur. Its Appl.*, vol. 10, no. 1, pp. 247–256, Jan. 2016, doi: 10.14257/ijsia.2016.10.1.23.
[77] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, Jul. 2021, doi: 10.3390/s21144759.
[78] M. K. S. Tan, S. Goode, and A. Richardson, "Understanding negotiated anti-malware interruption effects on user decision quality in endpoint security," *Behav. Inf. Technol.*, vol. 40, no. 9, pp. 903–932, Mar. 2020, doi: 10.1080/0144929x.2020.1734087.
[79] H. Shahriar, T. Klintic, and V. Clincy, "Mobile phishing attacks and mitigation techniques," *J. Inf. Secur.*, vol. 6, no. 3, pp. 206–212, 2015, doi: 10.4236/jis.2015.63021.
[80] K. S. Jones, M. E. Armstrong, M. K. Tornblad, and A. S. Namin, "How social engineers use persuasion principles during vishing attacks," *Inf. Comput. Secur.*, vol. 29, no. 2, pp. 314–331, Dec. 2020, doi: 10.1108/ics-07-2020-0113.
[81] T. R. Peltier, "Social engineering: Concepts and solutions," *EDPACS*, vol. 33, no. 8, pp. 1–13, Feb. 2006, doi: 10.1201/1079.07366981/45802.33.8.20060201/91956.1.
[82] M. A. Siddiqi, W. Pak, and M. A. Siddiqi, "A study on the psychology of social engineering-based cyberattacks and existing countermeasures," *Appl. Sci.*, vol. 12, no. 12, p. 6042, Jun. 2022, doi: 10.3390/app12126042.
[83] R. Zieni, L. Massari, and M. C. Calzarossa, "Phishing or not phishing? A survey on the detection of phishing websites," *IEEE Access*, vol. 11, pp. 18499–18519, 2023, doi: 10.1109/ACCESS.2023.3247135. https://doi.org/10.1109/access.2023.3247135
[84] A. A. Ubing, S. Kamilia, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "Phishing website detection: An improved accuracy through feature selection and ensemble learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 1–19, 2019, doi: 10.14569/ijacsa.2019.0100133.
[85] M. Uddin and D. Preston, "Systematic review of identity access management in information security," *J. Adv. Comput. Netw.*, vol. 3, no. 2, pp. 150–156, 2015.
[86] H. A. Aldawood and G. Skinner, "A critical appraisal of contemporary cyber security social engineering solutions: Measures, policies, tools and applications," in *Proc. 26th Int. Conf. Syst. Eng. (ICSEng)*, Dec. 2018, pp. 1–6, doi: 10.1109/ICSENG.2018.8638166.
[87] E. Stobert and R. Biddle, "The password life cycle," *ACM Trans. Privacy Secur.*, vol. 21, no. 3, pp. 1–32, Aug. 2018, doi: 10.1145/3183341.
[88] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud*, Aug. 2016, pp. 145–149.
[89] W. A. Cram, J. G. Proudfoot, and J. D'Arcy, "Organizational information security policies: A review and research framework," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 605–641, Nov. 2017, doi: 10.1057/s41303-017-0059-9.
[90] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102030, doi: 10.1016/j.cose.2020.102030.

[91] H. Haqaf and M. Koyuncu, "Understanding key skills for information security managers," *Int. J. Inf. Manage.*, vol. 43, pp. 165–172, Dec. 2018, doi: 10.1016/j.ijinfomgt.2018.07.013.
[92] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl, "Computer security incident response team development and evolution," *IEEE Secur. Privacy*, vol. 12, no. 5, pp. 16–26, Sep. 2014, doi: 10.1109/MSP.2014.89. https://doi.org/10.1109/msp.2014.89
[93] R. Van der Kleij, G. Kleinhuis, and H. Young, "Computer security incident response team effectiveness: A needs assessment," *Frontiers Psychol.*, vol. 8, pp. 1–27, Dec. 2017, doi: 10.3389/fpsyg.2017.02179.
[94] M. D. Ibrishimova, "Cyber Incident classification: Issues and challenges," in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 24. Cham, Switzerland: Springer, 2019.
[95] C. M. Patterson, J. R. C. Nurse, and V. N. L. Franqueira, "Learning from cyber security incidents: A systematic review and future research agenda," *Comput. Secur.*, vol. 132, Sep. 2023, Art. no. 103309, doi: 10.1016/j.cose.2023.103309.
[96] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" 2019, *arXiv:1901.02672*.
[97] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, pp. 65–78, Sep. 2015, doi: 10.1016/j.cose.2015.05.012.
[98] A. Alraizza and A. Algarni, "Ransomware detection using machine learning: A survey," *Big Data Cognit. Comput.*, vol. 7, no. 3, p. 143, Aug. 2023, doi: 10.3390/bdcc7030143.
[99] H. Aldawood and G. Skinner, "Challenges of implementing training and awareness programs targeting cyber security social engineering," in *Proc. Cybersecurity Cyberforensics Conf.*, May 2019, pp. 111–117.
[100] M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Comput. Hum. Behav.*, vol. 66, pp. 75–87, Jan. 2017, doi: 10.1016/j.chb.2016.09.012.
[101] W. Rocha Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," *Comput. Secur.*, vol. 59, pp. 26–44, Jun. 2016, doi: 10.1016/j.cose.2016.01.004.
[102] F. Mouton, M. M. Malan, K. K. Kimppa, and H. S. Venter, "Necessity for ethics in social engineering research," *Comput. Secur.*, vol. 55, pp. 114–127, Nov. 2015, doi: 10.1016/j.cose.2015.09.001.
[103] J. M. Hatfield, "Virtuous human hacking: The ethics of social engineering in penetration-testing," *Comput. Secur.*, vol. 83, pp. 354–366, Jun. 2019, doi: 10.1016/j.cose.2019.02.012.
[104] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, Sep. 2018.

MOHAMED ZAOUI received the M.Sc. degree in computer science from the Faculty of Sciences Agadir, Ibn Zohr University, Morocco, in 2012. He is currently pursuing the Ph.D. degree with Sultan Moulay Slimane University, with a research focus on cybersecurity.

BELFAIK YOUSRA received the master's degree in computer science, with a focus on telecommunications systems and computer networks from the Polydisciplinary Faculty of Beni Mellal, Sultan Moulay Slimane University, Morocco, in 2019. She is currently pursuing the Ph.D. degree, with a research focus on identity and access management systems, networks security and privacy, and blockchain.



SADQI YASSINE (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science, with a focus on computer security from the Faculty of Sciences Agadir, Ibn Zohr University, Morocco, in 2012 and 2015, respectively. From 2017 to 2021, he was an Assistant Professor with Sultan Moulay Slimane University. In February 2021, he became an Associate Professor. He is currently the African Research Center of Information Technology Cybersecurity Vice President. He has made contributions in the fields of web security, authentication protocols, network security, and cybersecurity. He has published several peer-reviewed research articles in international journals, book chapters, and conferences/workshops. He is a member of ACM Professional and OWASP. Furthermore, he has served and continues to serve on executive and technical program committees and as a reviewer of numerous international conferences and journals.

MALEH YASSINE (Senior Member, IEEE) received the Ph.D. degree in computer sciences management. He is currently an Associate Professor in cybersecurity and IT governance with Sultan Moulay Slimane University, Morocco. He is also the Founding Chair of IEEE Consultant Network Morocco and the Founding President of African Research Center of Information Technology Cybersecurity. He is a member of the International Association of Engineers IAENG and The Machine Intelligence Research Laboratories. He has published over 200 papers (book chapters, international journals, and conferences/workshops), 35 edited books, and six authored books. He is the Editor-in-Chief of the *International Journal of Information Security and Privacy* and the *International Journal of Smart Security Technologies* (IJSST). He serves as an Associate Editor for IEEE Access (2019 Impact Factor 4.098), the *International Journal of Digital Crime and Forensics* (IJDCF), and the *International Journal of Information Security and Privacy* (IJISP). He is a Series Editor of *Advances in Cybersecurity Management* (CRC Taylor Francis). He has served and continues to serve on executive and technical program committees and as a Reviewer of numerous international conferences and journals, such as *Ad Hoc Networks* (Elsevier), *IEEE Network Magazine*, IEEE Sensor Journal, *ICT Express*, and *Cluster Computing* (Springer). He was the Publicity Chair of BCCA 2019 and the General Chair of the MLBDACP 19 Symposium and ICI2C'21 Conference. He received Publons Top 1% Reviewer Award, in 2018 and 2019.

OUAZZANE KARIM (Senior Member, IEEE) received the Ingenieur D'etat degree (Hons.) in marine and mechanical engineering from the University of Oran, Oran, Algeria, in 1986, the M.Res. degree from the Department of Aerospace, Control and Mechanical Engineering, Liverpool University, Liverpool, U.K., in 1989, and the Ph.D. degree from the Department of Aeronautics, Manufacturing and Mechanical Engineering, Salford University, Greater Manchester, U.K., in 1994. He is currently a Professor in computing and knowledge exchange, the Director of Research and Enterprise, the Chair of European Cyber Security Council (Brussels), and the Founder of the Cyber Security Research Centre, London Metropolitan University, London, U.K. He has carried out research in collaboration with industry through a number of research schemes, such as The Engineering and Physical Sciences Research Council, KTP, EU Tempus, London Development Agency (LDA), and Knowledge Connect (KC). He has also authored or coauthored more than 100 articles, three chapters in books, is the author of three patents, and has successfully supervised 13 Ph.D. students. His research interests include artificial intelligence applications, bimodal speech recognition for wireless devices, cyber security and big data, computer vision, hard and soft computing methods, flow control and metering, optical instrumentation, and lasers. He is a member of the Oracle Corporation Advisory Panel.