Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 8, No. 2, April, 2024

Review Article

Common Techniques, Success Attack Factors and Obstacles to Social Engineering: A Systematic Literature Review

António Lopes [1*], Henrique S. Mamede [2, 3], Leonilde Reis [1], Arnaldo Santos [2, 3]

[1] *ESCE IPS - Polytechnic Institute of Setúbal, Setúbal, Portugal.*

[2] *Institute for Systems and Computer Engineering, Technology and Science (INESC TEC), Porto, Portugal.*

[3] *Department of Science and Technology, Universidade Aberta, Lisbon, Portugal.*

Abstract

Knowledge of Social Engineering is crucial to prevent potential attacks related to organizational Information Security. The objective of this paper aims to identify the most common social engineering techniques, success attack factors, and obstacles, as well as the good practices and frameworks that could be adopted concerning their mitigation. As an analysis methodology, a Systematic Literature Review was carried out. The findings revealed that the discussion about SE attacks has increased and that the most imminent threat is phishing. Exploiting human vulnerabilities is a growing threat when the attack is not carried out directly through technical means. There continue to be more technical attacks than non-technical attacks. Encouraging organizational security prevention, like training, education, technical controls, process development, defense in detail, and the development of security policies, should be considered mitigating factors for the negative impact of SE attacks. Most SE frameworks/models are focused on attack techniques and methods, mostly on technical components, decorating human factor. As a novelty, we found the opportunity to develop a new framework that could improve coverage of the gaps found, supported on security international standards, that could help and support researchers in developing their work, understanding open research topics, and providing a clearer understanding of this type of threat.

Keywords:

Social Engineering; Framework; Attack Techniques; Information Security; Organizations; Prevention; Information Systems; Human Behavior; Human Vulnerabilities; Persuasion Factors.

Article History:

Received:	20	November	2023
Revised:	22	March	2024
Accepted:	27	March	2024
Published:	01	April	2024

1- Introduction

Advances in digital communications have made communication between human beings more accessible and immediate. However, personal, and sensitive information may be available online through social networks and online services that do not have security measures to protect it. Information Security should be a strong concern for organizations, given the current context of business dependence on Information Systems (IS) and Information and Communication Technologies (ICT). The objectives of this work focus on the problem that organizations face with potential attacks using Social Engineering (SE) without even realizing it, with special emphasis on the human factor and its vulnerabilities. Instead of utilizing standard technological hacks to gain access to systems or networks, social engineering (SE) is the art of persuading employees to carry out a specified task for the attacker (such as divulging a password or providing confidential information about the organization) [1], cited by Wilcox & Bhattacharya [2]. Though definitions vary, it is generally accepted that SE entails studying human psychology to obtain private information. Emotions in people have the capacity to be both assets and liabilities. SE takes advantage of human weaknesses by using "traps" to play on human emotion and its fragility.

[*] **CONTACT**: antonio.jorge.lopes@esce.ips.pt

DOI: http://dx.doi.org/10.28991/ESJ-2024-08-02-025

Given the prevalence of Information Security breaches utilizing SE techniques, this is a problem that cannot be ignored [3]. SE is an increasingly present threat today, although it is already despised. In this sense, it is increasingly relevant that the managers and those responsible for IS recognize the importance of Information Security, worrying, in this specific context, to know which are the most used attack techniques, success factors, and obstacles in a potential attack of SE, as good practices that should be adopted concerning their mitigation.

Additionally, malevolent people can readily compromise communication systems through SE attacks, making them vulnerable. The goal of these attacks is to deceive people or organizations into doing things that will help the attackers or provide them access to private information. Because it takes advantage of the inherent human tendency, SE is one of the largest threats to network security. Simultaneously, humans are becoming an integral part of the system and playing a bigger role in IS due to the rapid growth of socio-technical systems. However, SE attacks have not been effectively addressed, in contrast to technological attacks that have been studied for decades [4].

Governments and businesses have made investments to guarantee the safety of private data and the confidence of their constituents. Technology alone is insufficient to prevent information theft. People are frequently the weakest link in an IS, and they can be persuaded or tricked into disclosing private information that gives unauthorized users access to systems that are protected [5]. From the same point of view, organizations are trying to keep an eye on and counteract hacker threats to Information Security, in addition to the growing sophistication of both technical and non-technical cyberattacks. Although numerous preventative strategies have been considered, created, and put into practice, the human factor is still the least understood and a major weak point in IS [6].

A social engineer employs a variety of strategies to take advantage of everyone's weaknesses to obtain access to private systems, confidential data, or money. One of the weakest points in any system's defense is its users. So-called cognitive distortions are the cause of the imperfections in the human brain. Attackers employ these distortions, sometimes called "errors in human thought" in a variety of ways to develop their attack strategies. Hackers examine the weaknesses of an individual or group of individuals with access to the required data. Later, they use the "weaknesses" found to gain the sensitive data or desired data, proving this to be the foundation of SE [7].

The human element is frequently disregarded, even if many cybersecurity specialists advise enterprises to employ defenses for their networks and Information Systems. The primary focus of security assessment frameworks is on the technical components of extant hazards and an organization's essential assets. As a result, there are insufficiently defined frameworks to recognize, classify, evaluate, and reduce the risks associated with SE [8]. In addition, SE refers to the "art" of persuading others to spread sensitive information, and the act of doing so is called a SE attack [5]. Based on this threat, it becomes relevant to understand how organizations can mitigate this type of attack. Thus, it is necessary to study and understand the various attack techniques and respective protection mechanisms, gaps in the literature, and the challenges for organizations and employees' prevention. However, a good signal is that research is increasing, and a range of previously published studies in the literature have explored the threat of SE attacks and proposed various frameworks and approaches to prevent and mitigate them.

A foundation for the advancement of security technique development is proposed in the Model for Security Threats and Attack Methods [9]. It is restricted to specific attack and vulnerability categories, but it addresses security both inside and outside the system to stop SE-based attacks. Although it emphasizes the IT-related components of SE attacks. A framework for evaluating and comprehending the viewpoints of employees while utilizing social networks to launch more successful education-based interventions was created by Albladi & Weir [10]. It does not, however, offer specific instructions on how these traits relate to vulnerability to SE attacks or how to reduce them. It is possible to augment the Framework by Albladi & Weir [10] with the user-centric framework's threat detection capacity elements [3] and vice versa. This research explores four different sorts of variables: psychological, perceptual, habitual, and emotional, allowing one to perceive human vulnerabilities. Along with some general avoidance advice, a defense cycle idea for SE attacks is offered.

Developed in contrast to earlier models that were filled with questions about SE attacks involving different forms of communication (unidirectional, bidirectional, or indirect), Mouton et al. [5] created the Finite State Machine for the Social Engineering Attack Detection Model. They argue that this offers a more thorough view of the implementation of mechanisms for detecting SE attacks. To facilitate decision-making, this approach uses a decision tree and divides the procedure into smaller, more manageable parts. Is expandable, and even though it can't fend off every kind of attack, it's still a positive development for the field of SE research.

A Critical Thinking Model for Security and Privacy was developed by Hamoud & Aïmeur [11]. It presents the Security Training Model (STRIM), a theoretical user-based security training model that attempts to inform and prepare users to recognize, steer clear of, and report cyberattacks in which they are the main target. The authors' suggested model might be able to assist organizations in encouraging security-conscious behavior among their staff members. Nevertheless, there isn't a single solution that can address every security risk. For instance, this approach might not be able to sufficiently handle the difficulties presented by complicated SE scenarios. The best example is zero-day attacks.

It places a strong emphasis on encouraging users to adopt security-conscious behaviors, but it could not offer enough technical training to enable users to identify and neutralize SE risks. Acquiring knowledge of the technical elements of prevalent attack vectors, including malware, phishing emails, and network flaws, is necessary for efficient mitigation and detection of SE threats.

Li et al. [12] have launched an initiative for a framework that includes a generic procedure for analyzing SE attacks. They provide an overview of several issues that impede SE research. They acknowledge that it is tough to investigate SE attacks given the list of difficulties, but they also think that their initial approach will be helpful for further research on SE. For addressing SE attacks, there isn't an effective security requirements analysis methodology. The unpredictability of human action is a significant barrier to solving this issue, making it challenging to evaluate SE attacks accurately.

Following the same line, a new approach for the SE Attack Analysis Framework is suggested by Yasin et al. [13]. It examines the social roles that attackers and victims play, the vulnerabilities that lie beneath the surface of the victims, the principles that attackers use to their advantage, and the narratives that the attackers create in relation to the current SE circumstances. Even yet, it's important to investigate situations in which the attacker failed to achieve their objective and determine why the attack didn't succeed.

A prediction framework is offered by Aldawood & Skinner [14] to help decision-makers get rid of insider threats to cyber security. Although this framework includes important insider threat indicators, it might not include all the indicators that could point to possible insider risks. To improve detection efficacy and accuracy, the framework might need to be broadened to include a wider variety of indicators. We should not forget the concept of cyber hygiene. In that sense, Esparza et al. [15] created a paradigm for modeling cyber hygiene. The goal is to improve self-assessment tool design so that businesses can develop better questionnaires that provide a deeper understanding of the respondent and make it possible to recognize different kinds of dangers and their underlying causes.

In addition to this, due to the level of complexity of attacks, to avoid threats, organizations invest mostly in protecting their infrastructure and network through systems such as antivirus, firewalls, and intrusion detection. On the other hand, it is desirable to complement the technical measures with the awareness of employees regarding the SE attack techniques used and the development of skills to identify and deal with them.

It is challenging to recognize and lessen SE attacks since they are associated with human emotions and behaviors. It is crucial to comprehend how this type of attack is put together as well as the methods attackers employ to find weaknesses in employees. All organizational levels—top, intermediate, and operational—should be included in employee education against SE attacks. Topics like workshops, training, awareness, simulations, and evaluations should be covered. In this sense, considering human vulnerabilities, our approach to filling the gaps is a new framework proposal that can help in the prevention, training, and preparation of employees while providing faster and more flexible recognition and response to the latest threats, becoming relevant for a more robust Information Security strategy in organizations. The goal of this model is to help resolve the literature gaps found in the domains of employee education and continuous improvement in terms of SE prevention and, at the same time, improve and aggregate them with SE techniques, international norms and standards, and types of targets.

Comprehending human weaknesses facilitates a more all-encompassing strategy for cybersecurity. Through the study of human vulnerabilities, cybersecurity professionals may remain on top of new threats, develop proactive tactics to mitigate risks before they are exploited, and gain a better understanding of how attackers leverage these qualities to achieve their nefarious purposes. This knowledge aids in the creation of stronger defenses against SE attacks.

Technical measures are important, but they are insufficient on their own. In addition to technical controls, human-centric security measures create a more robust security posture. Examples of these efforts include policy enforcement, awareness campaigns, and training. Understanding the relationship that exists between technology, human behavior, and cybersecurity requires an understanding of SE in terms of human weaknesses.

This article is structured as follows: In Section 2, a brief description of Barbara Kitchenham's protocol. The Execution of the Research Protocol in Section 3, where we identify the pertinence of this Systematic Literature Review (SLR), a summary of previous reviews found in the literature, and a mention of the research questions associated with this SLR, as well as the sources consulted, Strategies are defined, and the Conducting is in Section 4, where data extraction and synthesis are explained and criteria for inclusion or exclusion are presented. Section 5 presents the reporting of the results found in the literature and the respective gaps. Section 6 discusses the results relative to the initial ones, considering their differences in quality and results obtained. In Section 7, we propose an SE attack prevention framework for the organization's employees. In Section 8, the authors conclude with the practical implications of this literature review in the organizational context, unanswered questions, and research opportunities for future research. In the next section, we will present the research protocol used.

2- Brief Description of the Research Protocol

An SLR is "a way of evaluating and interpreting all available research relevant to a particular issue, research area, or phenomenon of interest" [16]. To do this research and to achieve the objectives of this study, a Systematic Literature Review (SLR), supported by the Barbara Kitchenham Protocol [16], was applied to locate, extract, and synthesize relevant information from the selected articles in the context of the theme mentioned above, based on the inclusion and exclusion criteria previously defined.

According to Bryant & Seok [17], cited by de Freitas et al. [18], SLR is a methodological review of research findings that seeks to compile the body of knowledge regarding a research issue and to find objectively and consistently pick, assess, and summarize primary publications that are thought to be pertinent to the topic of the study. SLR is regarded as a secondary research method for compiling earlier works. This protocol was carried out in three phases: planning, conducting, and reporting (Figure 1). This methodology was followed when using the web tool parsif.al, which was created to assist researchers in conducting systematic literature reviews.

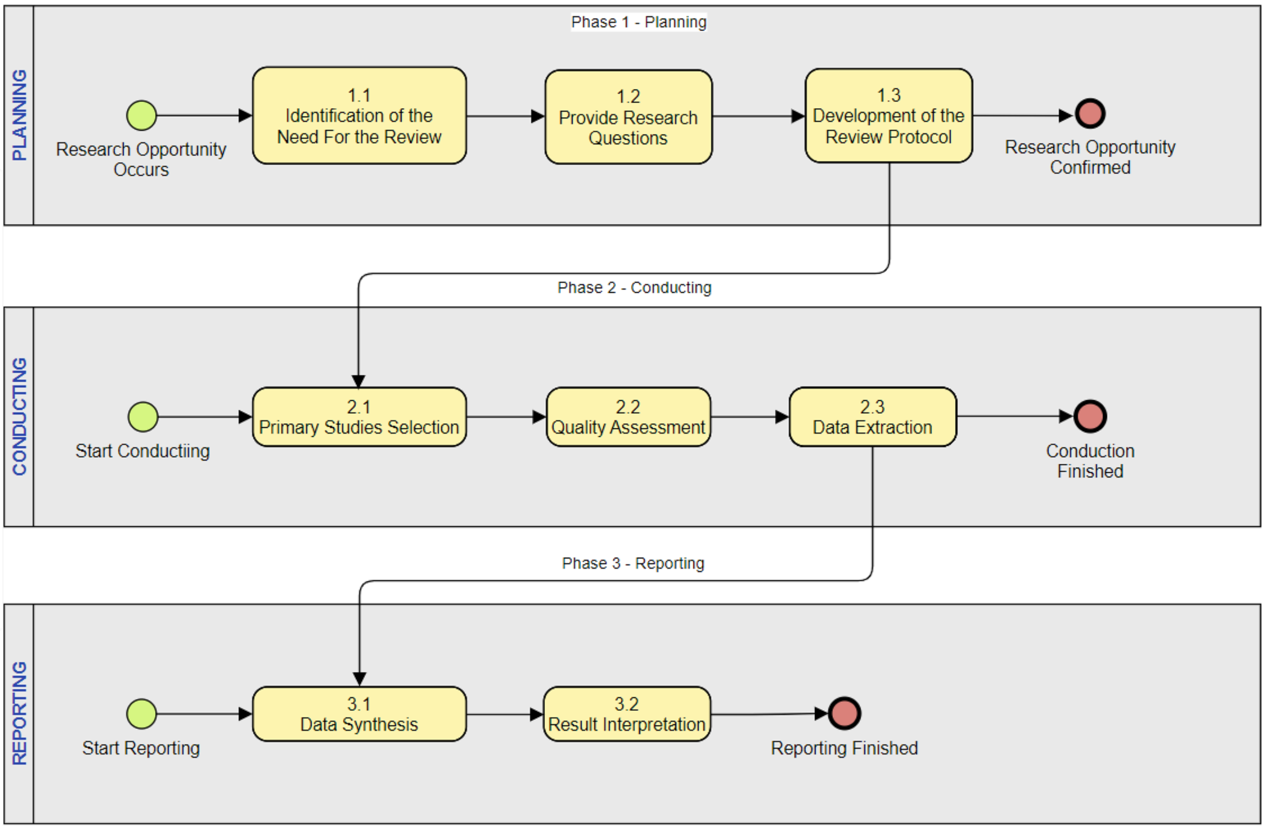
Phase 1 - Planning
PLANNING
Research Opportunity Occurs
1.1 Identification of the Need For the Review
1.2 Provide Research Questions
1.3 Development of the Review Protocol
Research Opportunity Confirmed
Phase 2 - Conducting
CONDUCTING
Start Conductiing
2.1 Primary Studies Selection
2.2 Quality Assessment
2.3 Data Extraction
Conduction Finished
Phase 3 - Reporting
REPORTING
Start Reporting
3.1 Data Synthesis
3.2 Result Interpretation
Reporting Finished

Figure 1. The systematic review steps (adapted from Kitchenham & Charters [19])

These three stages of the SLR protocol are outlined in Figure 1: the conducting step involves finding primary papers through search strategies, selecting papers using inclusion and exclusion selection criteria for papers, extracting data, and synthesizing data; the publication step involves defining the report, formatting the report, and evaluating the report. During the planning phase, these activities can be completed interactively [20]. In the next section, the execution of the protocol will be described.

3- Execution of the Research Protocol

3-1- Planning

As we have seen, the first phase of the SLR methodology consists of planning, where we identify the research objective of an SLR and where the respective research questions are defined.

3-1-1- Research Objective

The objective of this systematic review goes beyond providing an overview of the conceptual evolution of the concept of SE. It intends to find answers regarding the SE models and frameworks found in the literature. Also, we intend to identify the most common SE techniques, what factors contribute to the success of SE attacks, and what obstacles are placed in SE attacks. This research could help promote and systematize organizational knowledge in this area to prevent and reduce the number of attacks and encourage the continuous adoption of best practices in an organizational context.

3-1-2- PICOC

PICOC is a framework for outlining a research question's five components. The acronym PICOC stands for population (who), context (in what sort of organizations or conditions), comparison (compared to what), intervention (what or how), and outcomes (what are we trying to accomplish or better). In this situation, we have:

- Population – All types of organizations.
- Intervention – Promotion and systematization of organizational knowledge in Information Security.
- Comparison - Alternative methods, best practices, or frameworks that address SE attacks.
- Outcome - Reduce the number of SE attacks and encourage continued adoption of information protection measures.
- Context - Critical or important information for organizations.

As a result, this research plans to answer the questions referred to in Section 3.1.2.

3-1-3- Research Questions

In order to perform an SLR, it is necessary to address clear and answerable research questions rather than a general topic or problem of interest. In this case, the four research questions are listed below:

RQ.1. *Aims to identify the SE techniques most used by attackers to obtain confidential information. Organizations' dissemination and knowledge of these techniques allow them to adopt a prevention mechanism to keep confidential information safe, avoiding potential attacks.*

RQ. 2. *Aims to analyze and make known the factors that most contribute to the success of SE attacks. If organizations are familiar with these success factors, they will likely be more attentive and well-prepared to mitigate SE attacks.*

RQ.3. *Aims to provide knowledge regarding the obstacles referred to in the context of an SE attack. By being contextualized, organizations and their employees can apply this knowledge to prevent SE attacks.*

RQ.4. *Identifies SE attack prevention frameworks over the past two years. These frameworks can serve to train the employees of organizations or even for the development of new frameworks or improvements of existing frameworks.*

After defining the research questions, it becomes necessary to briefly describe the research process, the study selection criteria, the quality assessment criteria, data extraction, and results, which will be described in the next sections, before the execution of the protocol.

3-2- Conducting

To start this SLR, it was necessary to conduct searches in bibliographic databases (EBSCO, IEEE Digital Library, and SCOPUS) through a search string. In practice, using a search string allows us to perform a combination of keywords using logical operators, namely AND and OR. The keywords used in this SLR were social engineering, attack, threat, scenario, framework, approach, template, artifact, instrument, method, model, procedure, technique, prevent, detection, defense, protect, mitigation, information, Information Security, and organization. Several attempts were made to optimize the results returned by the searches. Each database returned a set of papers. These papers were imported into the Par-sif.al tool, and duplicates were removed. After removing the duplicate articles, the Study Selection was carried out.

3-2-1- Study Selection Criteria

After obtaining the set of papers mentioned above, it is necessary to define the inclusion and exclusion criteria to verify which papers meet the preconditions for acceptance or exclusion. The definition of these criteria is very useful and necessary to identify which papers will answer the research questions. There are inclusion criteria, which reinforce the paper's relevance to the investigation, and exclusion criteria, used to exclude papers that do not meet the research requirements. The next step consists of a Quality Assessment.

3-2-2- Quality Assessment

After the pre-selection of the previous set of papers, for them to be accepted for the SLR process, it is necessary to assess their quality. At this stage, each of the papers is evaluated to ensure that it is relevant to the answers to the research questions. In this context, a checklist with six questions was created to assess the quality of each of the papers.

Q1. Does it accurately identify the objectives?

Q2. Was it written to achieve the identified objectives?

Q3. Does it identify the methodology clearly, appropriately, and accurately?

Q4. Does it describe frequently used SE techniques, success factors, or obstacles to the success of SE attacks?

Q5. Does it demonstrate the main results or how to demonstrate them?

Q6. Is it possible to apply the results obtained outside the referenced context?

Each question has three options as answers, each with its respective score. Options are “yes”, “partially”, and “no”, scoring 1.0, 0.5, and 0, respectively. The total score for each paper was defined by the sum of the values obtained from six answers. A maximum value of 6.0 indicates a well-matched paper for this SLR, and a minimum of 0.0 indicates that the paper was unsuitable. A cutoff score of 2.5 was defined, so only papers with a score greater than 2.5 were effectively considered accepted for this SLR. This quality assessment method was implemented and applied using the tool Parsifal.

After this phase, a set of papers passed to the next stage, data extraction, which will be described in the next section.

3-2-3- Data Extraction

The data extraction process uses a data extraction form generated for this SLR using the Parsifal tool. Filling in the fields of this form after reading each selected paper allows for the extraction of pertinent data to answer the research questions raised by this SLR. After the data extraction, it is pertinent to show the investigation results through the steps described in Section 3.3.

3-3- Results

This section will summarize the findings and results of the analyses of the selected primary papers. The selection process was conducted in the selected databases. The papers that have been analyzed have relevant contributions to the research on SE prevention and mitigation. Next, in Section 4, the execution of this protocol in practice will be explained.

4- Conducting

The second phase of the SLR protocol is conducted. We start by defining the data sources and the search strategy.

4-1- Data Sources and Search Strategy

The need for a review was identified during planning, and the review protocol was clearly determined. In this article's case, the literature selection was based on search criteria (Table 1).

Table 1. Search criteria

Element	Research Details
Final Search String	("social engineering") AND (attack* OR threat* OR scenario*) AND (framework* OR approach* OR template* OR art?fact* OR instrument* OR method* OR model* OR procedure* OR techn*) AND (prevent* OR detect* OR defens* OR protect* OR mitig*) AND (information OR "information security") AND (organisation*).
Search Strategy	Articles in academic journals, conference materials, book, book chapters, master’s dissertation, and doctoral thesis between year 2016 and begin of year 2022.
Results	2742

After the data sources and search strategy are defined, it is necessary to define the selection of the articles for the study, which occurs according to a given inclusion and exclusion criteria. Once the final articles were selected, data extraction, monitoring, and synthesis occurred. To obtain the final set of papers, several filtering stages were executed over the first set of 2747 papers collected (Figure 2).

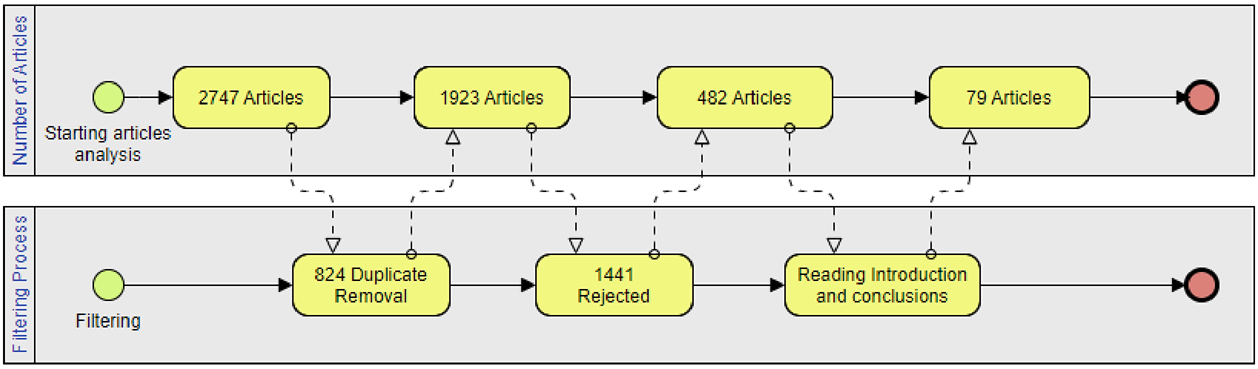

Figure 2. Article filtering process

Following the article's filtering process in Figure. 2, it is important to refer to the inclusion and exclusion criteria. The titles and abstracts of these papers were read, which led to classifying them into two types:" accepted", "partially", and "rejected". To obtain the final set of articles, it was necessary to perform a filtering process. Thus, from the initial set of 2747 articles obtained, 824 duplicate articles were removed, resulting in 1923 articles. Of these, titles and abstracts were analyzed. For summaries that raised doubts, they were downloaded, analyzed, and accepted or not for qualification.

Following the analysis of the titles and reading the abstracts, 1441 articles were excluded because they did not comply with the inclusion and exclusion criteria, resulting in 482 articles for analysis. Then, the respective introductions were analyzed, making it possible to infer greater detail from the objective of each study. In this sense, of the excluded articles, most did not fit the research context, were based on courses, had no publication in scientific journals, conference minutes, or peer review, or were inaccessible publications.

In the end, a set of 79 articles from different journals and academic conferences were accepted and evaluated, 8 of which were based on literature reviews: 33 from journal papers (Table 2), 33 from conference papers (Table 3), and 8 complementary publications of different types (Figure 3).

Table 2. **Number of publications (Journals)**

Journals	Number of Publications
Information Security for South Africa	1
ACM Computing Surveys	1
Computers & Security	1
Computers and Electrical Engineering	1
Computers in Human Behavior Reports	1
Computer Science Review	1
Frontiers in Computer Science	1
Human-Centric Computing and Information Sciences	1
Information & Computer Security	1
Information Systems	1
International Journal of Advanced Computer Research	1
International Journal of Advanced Computer Science and Applications	1
International Journal of Computer Network & Information Security	1
International Journal of Digital Crime and Forensics	1
International Journal on Cybernetics & Informatics	1
Issues in Information Systems	1
Journal Administrasi Kesehatan Indonesia	1
Journal Cybersecurity	1
Journal Future Internet	2
Journal Healthdatamanagement.com	1
Journal IEEE Access	4
Journal Information	1
Journal Ingineria socială - noul joc al înşe.lăciunii	1
Journal of Business & Psychology	1
Journal of Investigative Psychology & Offender Profiling	1
Journal of Organizational & End User Computing	1
Journal of Systemics, Cybernetics and Informatics	1
Memoirs of the Scientific Sections of the Romanian Academy	1
Security & Privacy	3

It is possible to observe in Table 2 that the journal with the most publications in this context is Journal IEEE Access, with four, followed by Security and Privacy with three, and Journal Future Internet with two. All others have one publication.

In Table 3, we can observe the number of publications by conference.

Table 3. Number of publications (Conference Papers)

Conferences	Number of Publications
AHFE International Conference on Human Factors in Cybersecurity	1
Annual Computing and Communication Workshop and Conference (CCWC)	1
Annual Ubiquitous Computing, Electronics and Mobile Communication Conference	1
Conference on Cryptography, Security and Privacy	1
Conference on Cyberworlds	1
Conference on Human Factors in Cybersecurity	1
Conference on Industrial Electronics and Applications	1
Cybersecurity and Cyberforensics Conference	1
Ethical Hacking Conference	1
International Requirements Engineering Conference	1
International Conference on Future Internet of Things and Cloud	1
Information and Communication Conference	1
Information Security for South Africa Conference	1
Integrated STEM Education Conference	1
International Carnahan Conference on Security Technology	2
International Conference for Internet Technology and Secured Transactions	1
International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability	1
International Conference on Computing Frontiers	1
International Conference on Computing, Communication and Automation	1
International Conference on Cyber Security & Protection of Digital Services	1
International Conference on Cyber Situational Awareness, Data Analytics and Assessment	2
International Conference on Electro-Information Technology	1
International Conference on Emerging Technologies	1
International Conference on Engineering Technologies and Applied Sciences	1
International Conference on Future Internet of Things and Cloud Workshops	1
International Conference on Reliability, Infocom Technologies and Optimization	1
International Conference on Teaching, Assessment, and Learning for Engineering	1
International Conference Proceeding Series	1
International Symposium on Digital Forensics and Security (ISDFS)	1
IST-Africa Conference	1
National Computing Colleges Conference, National Computing Colleges Conference	1
SAI Computing Conference	1
Science and Information Conference	1
Ural Symposium on Biomedical Engineering, Radio Electronics, and Information Technology	1

In this case, the two conferences with more publications in this context are the Integrated STEM Education Conference and the International Conference on Cyber Situational Awareness, Data Analytics, and Assessment. All the other conferences have one publication. Also, in this SLR, other types of publications were used (Figure 3).

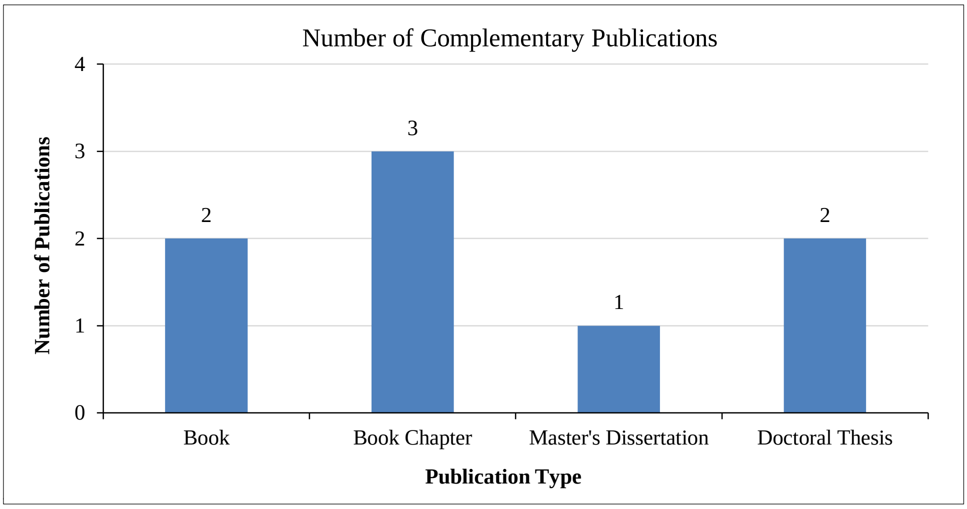

Figure 3. Complementary types of publications

These complementary publications were relevant to this investigation, using two books, one book chapter, one master's dissertation, and a doctoral thesis. Through the previous three figures, we have found that there aren't many academic studies on ways to stop SE attacks in organizations. There can be several reasons for this. If we compare SE as a field of study to other areas of Information Security, it is not as old. Although the concept has been around for decades, formal recognition as a discipline and scientific investigation into it are relatively new.

SE involves a cross-section of several disciplines, such as psychology, computer science, Information Security, and communication. This makes research in this field challenging and necessitates a multidisciplinary approach. In some cases, there may be a lack of incentives for academic researchers to focus on this topic. This can occur if there is a perception that the topic is not sufficiently "technical" or "scientific" enough to attract funding or publications in prestigious journals. There might not always be enough motivation for scholars to concentrate on this subject. This could happen if it's thought that the subject isn't "technical" or "scientific" enough to garner money or papers in esteemed journals. However, as awareness of the importance of Information Security increases and incidents of SE become more prominent, there is likely to be an increase in research and the publication of scientific articles on measures to prevent these attacks. In Figure 4, the number of articles (publications) per subject can be analyzed within the SE problem.

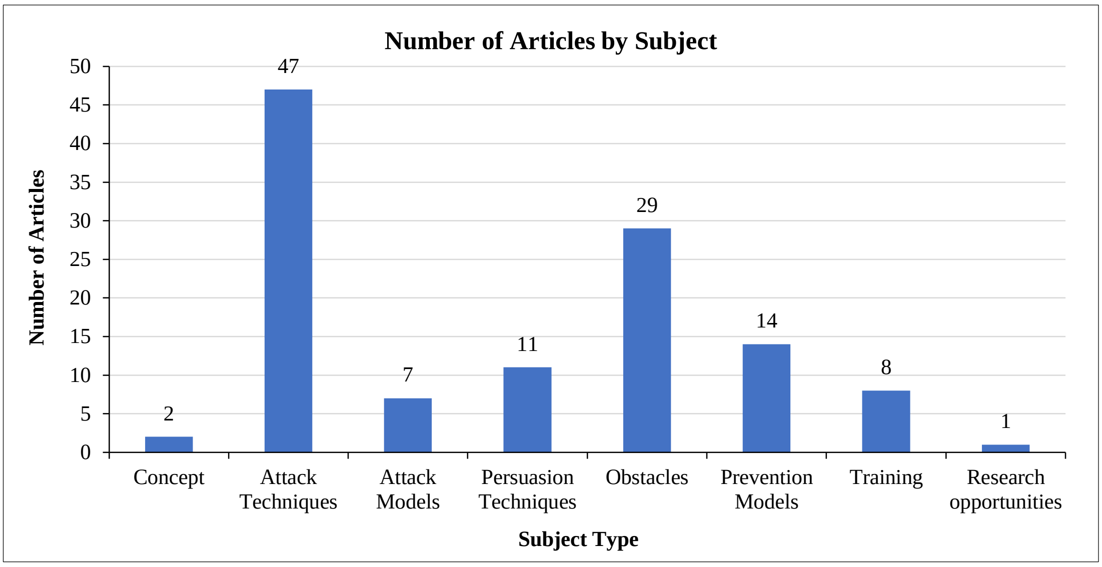

Figure 4. Number of articles by subject

To complement the information mentioned above, in Table 4, we present the title of each article with the subjects addressed.

Table 4. Title by subject

Title	Subject(s)
Social engineering 2.0: A foundational work	Attack Techniques
Social Engineering: The Art of Attacks	Attack Techniques
The awareness of social engineering in information revolution: Techniques and challenges	Attack Techniques
Social Engineering Attack Strategies and Defense Approaches	Attack Techniques; Obstacles
A literature survey on social engineering attacks: Phishing attack	Attack Techniques
The social engineering attack spiral (SEAS)	Obstacles, Prevention Models
A layered defense mechanism for a social engineering-aware perimeter	Attack Techniques; Obstacles
Benchmarking a mobile implementation of the social engineering prevention training tool	Prevention Models
Underlying finite state machine for the social engineering attack detection model	Prevention Models
A preliminary radicalisation framework based on social engineering techniques	Persuasion Techniques
Social Engineering: Application of Psychology to Information Security	Persuasion Techniques
An Overview of Social Engineering in the Context of Information Security	Attack Techniques; Prevention Models
Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review	Obstacles
Why Ransomware Needs a Human Touch	Attack Techniques
A Human Vulnerability Assessment Methodology	Attack Techniques
Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering	Training
Towards Effective Assessment for Social Engineering Attacks	Prevention Models
Identification and prevention of social engineering attacks on an enterprise	Attack Techniques

Social Engineering Attacks A Reconnaissance Synthesis Analysis	Attack Techniques; Obstacles
A social engineering awareness and training workshop for STEM students and practitioners	Training
Social Engineering-Based Cyber-Attacks in Kenya	Attack Techniques
Analysis of Social Engineering Attack on Cryptographic Algorithm	Attack Techniques
Social Engineering: The Looming Threat	Attack Techniques; Obstacles
Understanding Responses to Phishing in Saudi Arabia via the Theory of Planned Behavior	Attack Techniques; Persuasion Techniques
The Main Social Engineering Techniques Aimed at Hacking Information Systems	Attack Techniques
A Taxonomy of Attacks and a Survey of Defense Mechanisms for Semantic Social Engineering Attacks	Attack Techniques
Towards an Automated Recognition System for Chat-based Social Engineering Attacks in Enterprise Environments.	Obstacles
Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools	Attack Techniques; Concept
Learn Social Engineering: Learn the Art of Human Hacking with an Internationally Renowned Expert	Obstacles; Training
Social Engineering: Hacking Systems, Nations, and Societies	Attack Techniques; Obstacles; Training
Protection Against Semantic Social Engineering Attacks	Attack Techniques; Prevention Models
Defense methods against social engineering attacks	Obstacles
Social engineering attack examples, templates and scenarios	Attack Models; Obstacles
Privacy-aware detection framework to mitigate new-age phishing attacks	Attack Techniques
An interdisciplinary view of social engineering: A call to action for research	Persuasion Techniques
Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model	Research Opportunities
A Taxonomy of Social Engineering Defense Mechanisms	Attack Techniques
User characteristics that influence judgment of social engineering attacks in social networks	Attack Techniques
Social engineering defense mechanisms and counteracting training strategies	Obstacles; Training
Aligning social concerns with information system security: A fundamental ontology for social engineering	Attack Techniques; Persuasion Techniques; Training
Social Engineering Attack Detection Model: SEADMv2	Training; Obstacles
Social engineering attack detection and data protection model (SEADDPM)	Prevention Models
Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks	Concept; Attack Techniques
Coronavirus social engineering attacks: Issues and recommendations	Attack Techniques; Obstacles
Social Engineering: I-E-based Model of Human Weakness for Attack and Defense Investigations	Attack Techniques; Persuasion Techniques
The impact of social engineer attack phases on improved security countermeasures: Social engineer involvement as mediating variable	Obstacles
A engenharia social e os perigos do phishing	Obstacles
Cybersecurity Inertia and Social Engineering: Who is Worse, Employees or Hackers?	Attack Models
Social Engineering as an Evolutionary Threat to Information Security in Healthcare Organizations	Attack Techniques, Persuasion Techniques, Obstacles
Social engineering in cybersecurity: a domain ontology and knowledge graph application examples	Attack Techniques; Obstacles
Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues	Attack Techniques; Obstacles
Social Engineering Attacks: A Survey	Obstacles
Social engineering attacks are still rising, as hackers become cagey: A new report says social engineering attacks are on the rise, with hackers using more spoofed phishing and HTTPS encryption in URL-based attacks.	Attack Techniques; Prevention Models
A Multivocal Literature Review on Growing Social Engineering-Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions	Attack Techniques
A Session and Dialogue-Based Social Engineering Framework	Attack Techniques; Obstacles
Defining Social Engineering in Cybersecurity	Attack Techniques
Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods	Attack Techniques e Attack Models
Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model	Attack Techniques; Attack Models; Persuasion Techniques
Social engineering as the new deception game	Persuasion Techniques
Organizational science and cybersecurity: abundant opportunities for research at the interface.	Attack Techniques; Persuasion Techniques
On the anatomy of social engineering attacks - A literature-based dissection of successful attacks.	Attack Techniques
A Risk Analysis Framework for Social Engineering Attack Based on User Profiling	Attack Techniques
On Social Engineering Attacks and Unintended Data Disclosures: Two Major Categories of End-User Cybersecurity Error	Attack Techniques
A multiple-perspective approach for insider-threat risk prediction in cyber-security	Attack Techniques
Considerations on Preventing Social Engineering over the Internet	Attack Techniques; Attack Models
An academic review of current industrial and commercial cyber security social engineering solutions	Attack Techniques
Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors	Attack Models

A framework to mitigate social engineering through social media within the enterprise	Obstacles
Exploring Effects of Organizational Culture upon Implementation of Information Security Awareness and Training Programs within the Defense Industry Located in the Tennessee Valley Region	Obstacles; Prevention Models
Social Engineering Defense Mechanisms: A Taxonomy and a Survey of Employees' Awareness Level	Obstacles; Prevention Models
Contemplating social engineering studies and attack scenarios: A review study.	Obstacles; Prevention Models
Overview of phishing landscape and homographs in Arabic domain names	Attack Techniques
Understanding and deciphering social engineering attack scenarios	Obstacles; Prevention Models
Redefining the Approach to Cybersecurity	Attack Techniques
Impact Analysis and Performance Model of Social Engineering Techniques	Attack Techniques; Attack Models
An Expert System as an Awareness Tool to Prevent Social Engineering Attacks in Public Organizations	Obstacles; Prevention Models
Social Engineering Penetration Testing within the OODCA Cycle - Approaches to Detect and Remediate Human Vulnerabilities and Risks in Information Security	Obstacles; Prevention Models
Social Engineering Incidents and Preventions.	Attack Techniques; Persuasion Techniques
A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises	Obstacles; Training

Through Figure 4 and Table 4, it is possible to observe that attack techniques determine the most discussed subject in the literature, followed by obstacles, prevention models, and persuasion techniques. Moreover, given the current increase in this type of attack on organizations, it seems that the number of scientific articles that present and discuss this problem is still quite small.

Because attack strategies pose direct risks to security, they are frequently the focus of literary works. We found that to keep up with emerging SE threats, researchers and practitioners frequently place a high priority on understanding attack strategies. They can create more effective defense and response plans if they comprehend the attackers' techniques. The type and publishing year of selected articles for the literature review are presented (Figure 5).

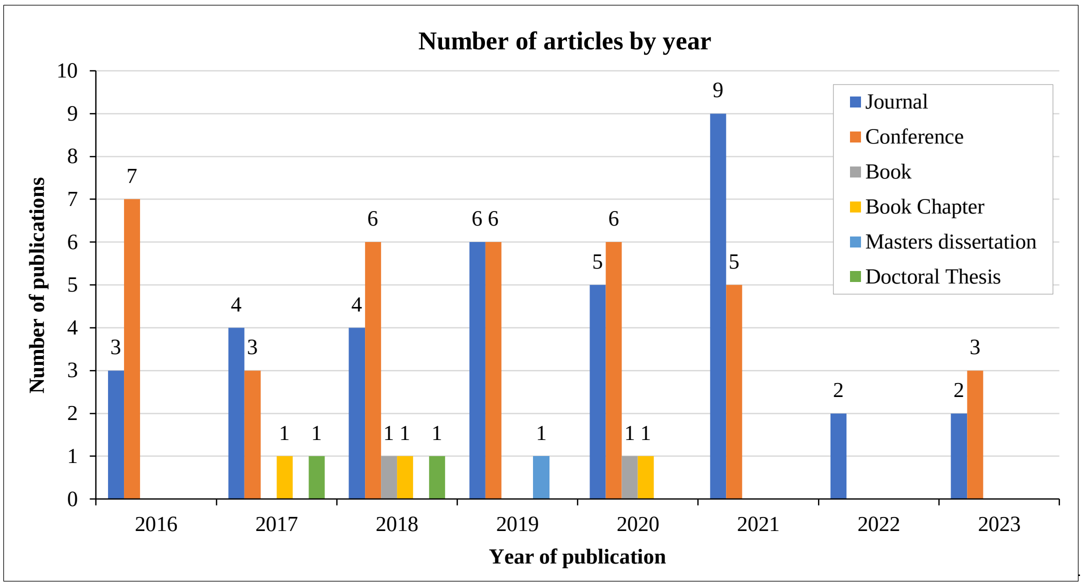

Figure 5. Type and publishing year of selected articles for literature review

As a result of the search, 8 literature reviews were found [14, 21–26]. In this section, a summary is made about its content so that the results can be analyzed and compared to this work.

The first study, conducted by Hijji & Alam [21], was to analyze the most advanced SE tactics, attack strategies, and attack platforms employed in the last two years of the pandemic to execute these attacks. 52 articles in all were analyzed. Thus, it was determined that the most common sociotechnical methods—false emails, websites, and mobile applications—in conjunction with phishing, scamming, spam, smishing, and vishing were the primary SE techniques employed during the COVID-19 pandemic. Ransomware, trojans, and bots are three forms of malware that are frequently used to compromise systems and resources.

In the second study, conducted by Yasin et al. [22], a review of the literature on SE was undertaken in numerous publications and notable conferences. There was mention of various attack and persuasion strategies employed by social engineers. The authors synthesized several theories that investigators attempted to apply to account for the diverse actions of social engineers. It is claimed that game-based theme analysis tools can help one understand SE assault scenarios better.

The objective of the third paper by Borkovich & Skovira [23] is a critical analysis of recent research and an exploratory story that, because it relates to SE, is restricted to the most pertinent instances of organizational inertia in the context of cybersecurity. It will go through its definition, history, present foundations and vulnerabilities, and potential future impact on enhancing networks, Information Systems security, and sensitive data in the workplace. It is feasible to examine suggestions to prevent cybersecurity inertia and mitigation techniques to keep SE threats inside enterprises in this review.

The fourth study, conducted by Wang et al. [24], defines the original meaning of SE in cybersecurity by a thorough analysis of the literature. Conceptual issues are addressed as the writers methodically analyze technical advancement and conceptual evolution. His study attempts to address these conceptual shortcomings by putting forth the more accurate and compatible definition of SE that is mentioned in the introduction. The objectives of this definition are to minimize generalization, cover traditional conceptual connotations, reduce conceptual inconsistencies, and define the conceptual border.

In the fifth study conducted by Aldawood & Skinner [14], several cybersecurity risks have been found in several settings. Exploiting human vulnerabilities as the weakest security link in these situations has raised user awareness of Information Security, in contrast to system technical flaws and protocols. Putting people through efficient training and education programs is one of the easiest fixes. This report explains how creative Information Security training programs can decrease cybersecurity incidents and effectively increase user/employee awareness.

In the sixth study, already in the context of a taxonomy for SE attack defense mechanisms [25], they created an SLR by selecting articles with "social engineering" in the title. They then identified the primary goals of social engineers and offered recommendations for countermeasures.

In the seventh identified study, a general knowledge extraction about SE was performed by Yasin et al. [13], using grounded theory, including attack vectors, psychological concepts, information gathering techniques, and attack cycles. To (a) comprehend the reasoning behind social engineers, (b) gather information about SE attacks and extract crucial details from sources, and (c) propose a framework to prevent SE attacks and how it can be used in security and training, they planned to review and synthesize a knowledge base (motivation of social engineers). It examines the current SE scenarios in terms of the social roles that attackers and victims play, the weaknesses that the victims have, the attackers' exploitation of certain principles, and the attackers' narratives.

The latest study is about SE on social networks. Chetioui et al. [26] provide and validate a user-centered framework that is built on four viewpoints: perceptual, habitual, sociopsychological, and socio-emotional. Prior studies typically focus on certain facets of these viewpoints that haven't been integrated into a single model to provide a more comprehensive knowledge of user susceptibility. While being aware of attack techniques is important, being able to successfully stop these attempts is what really makes one resilient to SE. If appropriate defense mechanisms are not put in place, organizations may become vulnerable if they just concentrate on the attack element. Organizations can create proactive techniques to detect, mitigate, and respond to possible attacks before they cause major damage by allocating resources towards research on SE prevention. This entails strengthening the organization's security posture through the implementation of preventative measures, in addition to comprehending how attacks happen. After this analysis, it is also important to know the relationship between the various keywords in the articles included in this SLR to have a perception of those that appear more frequently in the literature, as well as the strength of the link between them over the various articles that were analyzed.

For this analysis, the bibliographic data of the articles was loaded into the VOSviewer tool, an application that allows statistics to be extracted from the bibliometric analyses carried out. We can observe the relationship between the keywords. The type of analysis used was co-occurrence, where the relatedness of keywords is determined based on the number of documents in which they occur together. The unit of analysis is the number of keywords with a full counting method. In the selected articles, 177 keywords were found, with a minimum threshold of 2 occurrences (Figure 6).

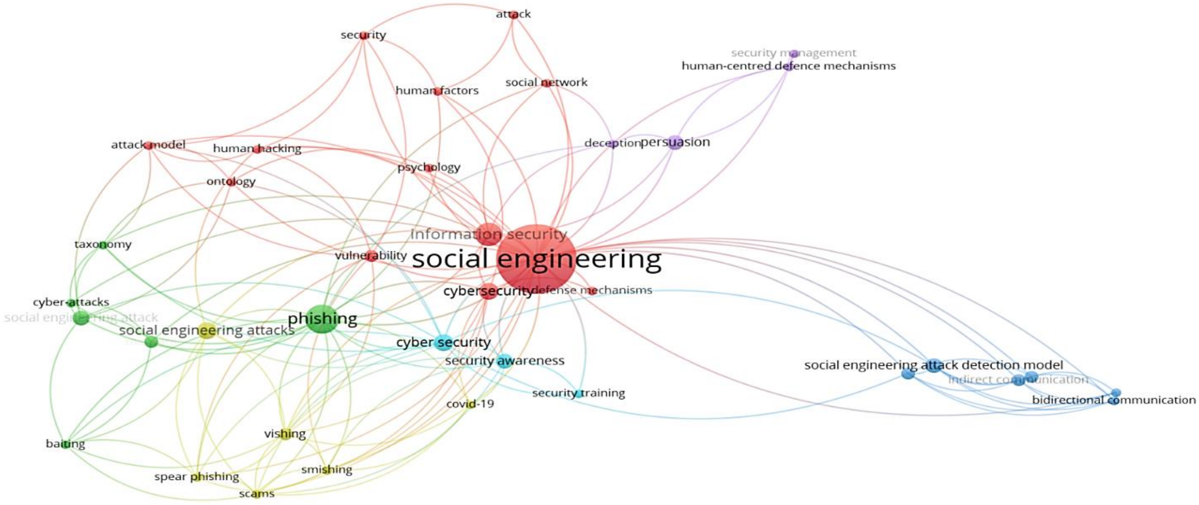

Figure 6. Co-occurrence map for all keywords

As a result, 38 keywords were analyzed to meet the threshold. The other ones consist of keywords that appear in isolation and, for this reason, were not considered for this visualization. For each of the 38 keywords, the total strength of the co-occurrence links with other keywords was calculated. The keywords with the greatest total link strength were selected and are represented in Figure 6.

Once again, the midterm, 'social engineering', appears more frequently. Also, we can represent the same data. However, in table format (Table 5), it is possible to identify each keyword, the number of occurrences in the related articles, and the strength of the link.

Table 5. Number of occurrences and total link strength of each keyword

Keyword	Occurrences	Total link strength
attack	2	5
attack model	2	8
baiting	2	9
bidirectional communication	2	11
covid-19	2	8
cyber security	5	18
cyber-attacks	2	6
cybersecurity	5	17
deception	2	6
defense mechanisms	2	4
human factors	2	6
human hacking	2	6
human-centred defense mechanisms	2	6
indirect communication	3	15
information security	8	16
malware	3	8
ontology	2	6
persuasion	4	10
phishing	11	39
psychology	2	4
scams	2	13
security	2	7
security awareness	4	14
security management	2	6
security training	2	5
smishing	2	12
social engineering	39	84
social engineering attack	4	10
social engineering attack detection model	4	18
social engineering attack examples	2	11
social engineering attack framework	3	13
social engineering attacks	5	8
social network	2	6
spear phishing	2	11
taxonomy	2	7
unidirectional communication	3	15
vishing	3	18
vulnerability	3	10

The two previous perspectives allow us to conclude that the term 'social engineering' is the one that comes up most frequently. Next, the 3 keywords that come up most frequently are 'phishing', 'cyber security' and 'Information Security'.

We found that these keywords provide insightful viewpoints on the prevailing SE and Information Security-related issues and concerns within the academic and research community. 'Phishing' is the most prominent keyword, highlighting the general worry about this specific kind of SE attack. The scientific community's interest in comprehending this prevalent form of attack is indicated by its prevalence.

The necessity of safeguarding systems and data from cyber-attacks and upholding the confidentiality, integrity, and availability of information is reflected in the terms "cyber security" and "Information Security." These words point to a more comprehensive approach to Information Security, covering a range of topics like risk management, data and network protection, regulatory compliance, and SE attack prevention. This identifies the primary areas of focus and interest.

After analyzing the links between keywords, it is relevant to know about another graphical element analysis that is very important, which corresponds to the network links between the various authors of the analyzed articles and shows the most outstanding.

After loading the same data used previously, related to the articles used in this SLR, 790 similar articles were found, that is, in the same research area, using the Research Rabbit tool. Of these 790 articles, the most relevant authors of this SLR were extracted, and they were related to the 40 most relevant authors in this research area (Figure 7).

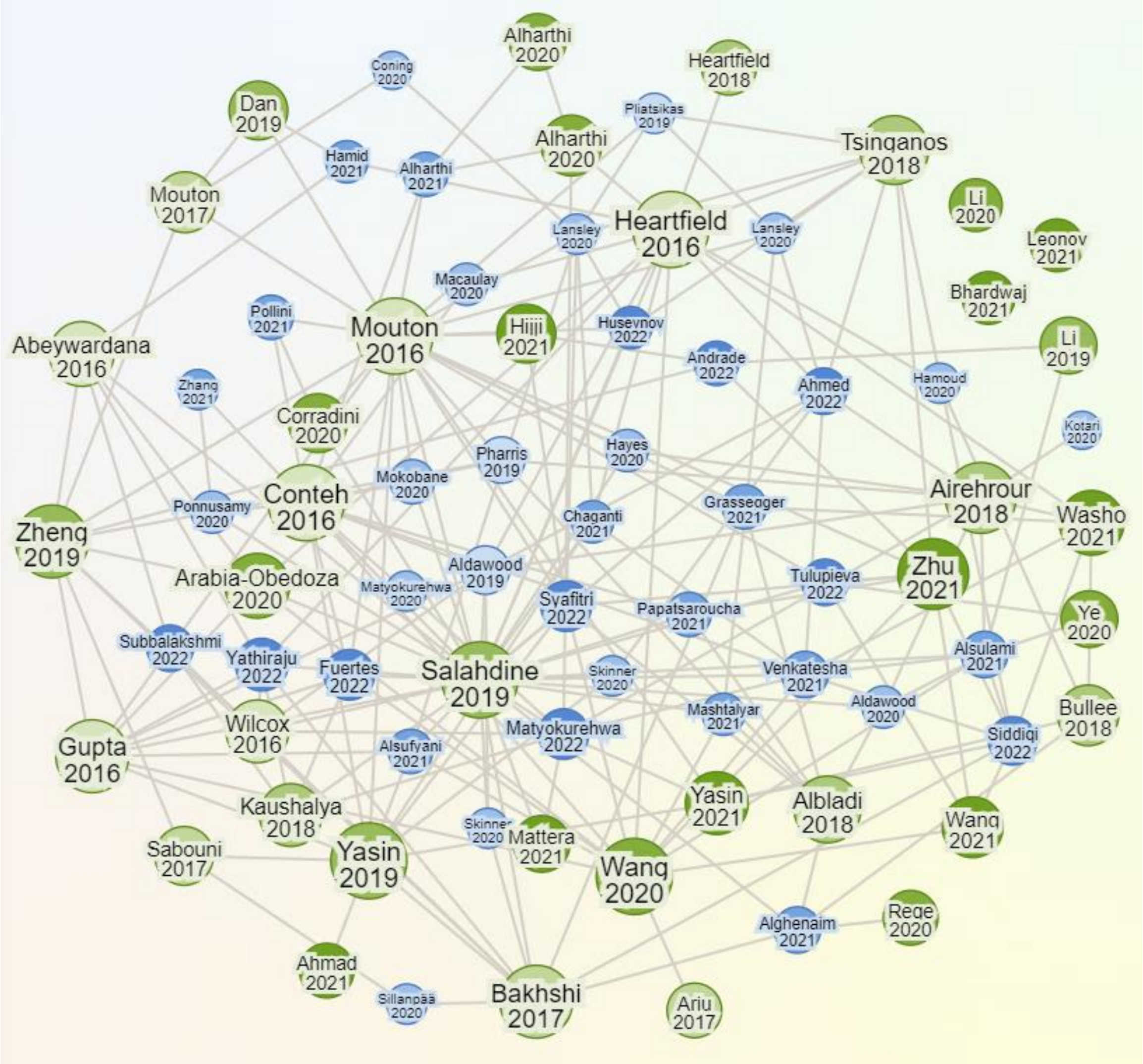

Figure 7. Similar work and author relationship

In green, the most relevant authors of this SLR and their relevance are identified according to the size of the circumference. We can also see the existing relationship of these authors with others from the same research area, identified in blue, present in other published articles (Figure 8).

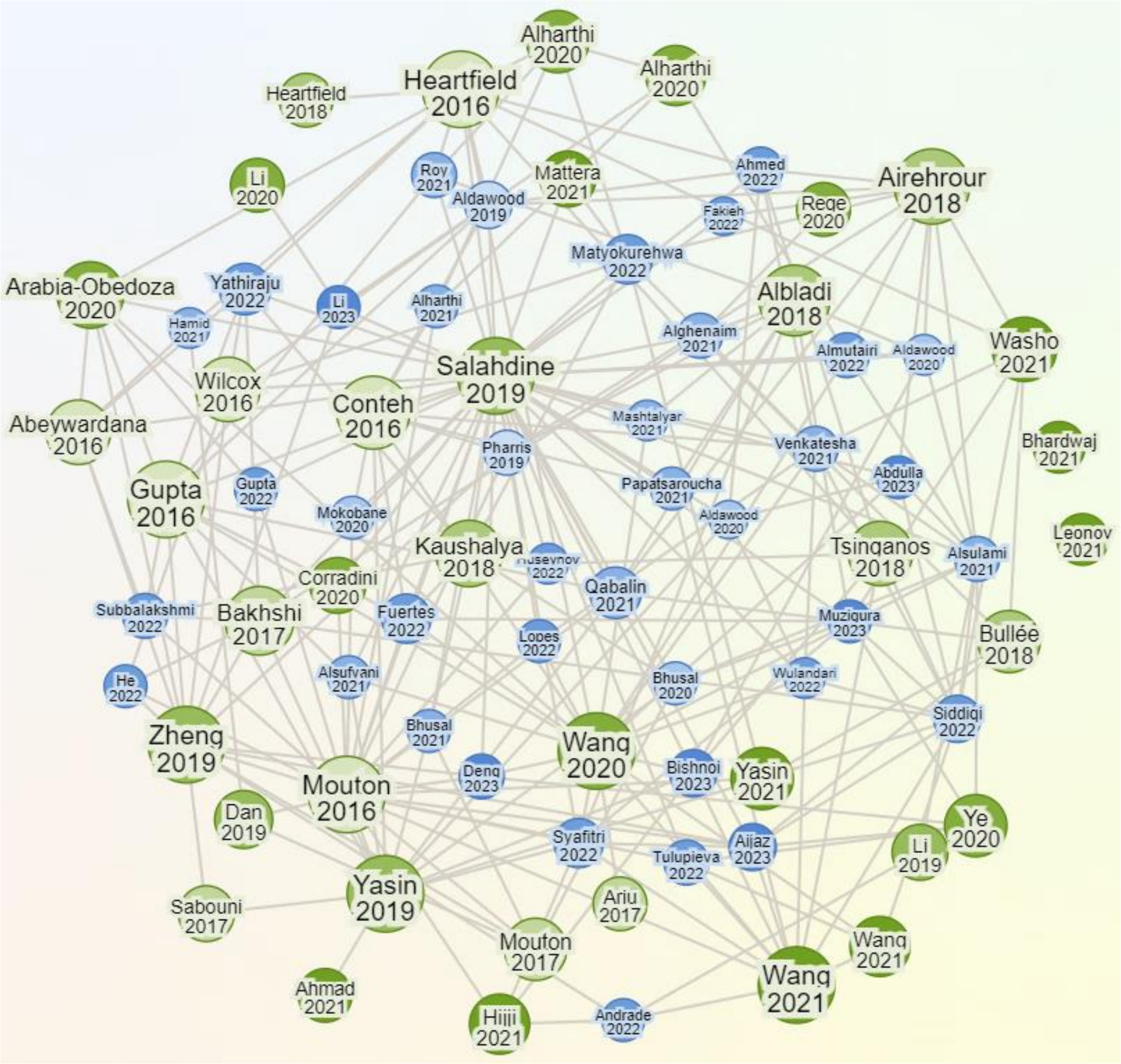

Figure 8. Later work and author relationship

It is possible to identify the authors already mentioned in this SLR through the green circles and their relevance according to the size of the circumference. It can be seen from this visualization that new authors with more recent publications are beginning to emerge, and that the area of research related to SE is growing.

Another conclusion we can draw is that the new authors are related to the authors cited in this SLR, and the lines of investigation are practically the same as those referred to in this article, related to attack techniques, attack and prevention models, and persuasion factors. The next section will present the results obtained through the analysis of the articles related to this SLR.

5- Reporting

In this section of the paper, answers to the research questions will be provided according to what was found when reading and analyzing the different articles.

5-1- RQ.1: What Are the Most Common SE Techniques?

During the analysis of the selected articles, we found that the most often employed SE tactics by the attackers could be found in the literature. It's interesting to observe in this context that there has been more talk regarding SE attacks via social networks. Organizational Information Security professionals face a wide range of people, process, and technology-related difficulties because employees are using social networks more and more at work. Because social engineers often use social engineering to target employees and attack an organization's information assets, businesses are concerned about SE attacks via social networks [2].

An organization's network can be readily infiltrated by the online hazards that social media platforms like Facebook and Twitter present to individuals, thanks to policies like bring-your-own-devices and insecure public data networks.

Additionally, there is a growing trend in social networks for SE techniques that address behavioral vulnerabilities resulting from the transversality of organizational security. The primary focus of SE online is on interactions between employees via social networks, utilizing strategies like baiting and befriending. Important losses for businesses include damage to their brand and/or legal liabilities resulting from unintentionally disclosing private information, publishing offensive content, or inadvertently infecting their networks with malware or viruses [2].

Working in a demanding atmosphere where judgments must be made quickly makes it more difficult to detect a SE attack. Because of this, it is imperative that the psychological and technological views of SE be carefully and properly analyzed. This is because they are essential to the preservation of Information Security in any community, individual, organization, or governmental agency [3].

As previously said, it is challenging to recognize and lessen SE attacks since they are associated with human emotions and behaviors. It is crucial to comprehend how this attack is put together as well as the methods attackers employ to find weaknesses in people. The two primary vulnerabilities that are exploited are psychological and physical. Attacks carried out physically reveal "where" or "how" attackers carry out their approach technique. Conversely, psychological elements take advantage of people's emotional and trusting weaknesses. Attackers take advantage of these human qualities to establish trusting bonds with their victims [3].

In the study conducted by Gupta et al. [9], the SE attacks have been linked to several important variables, including technology, security awareness, human, psychological, and emotional exploration, as well as the types of attacks. The most popular attacks utilized in most sectors are SE and hacking. The identified technical SE techniques are listed and displayed (Table 6).

Table 6. SE Technical techniques

Technical SE Technique	Sources
Baiting	[2, 3, 8, 9, 22-25, 27-38]
Bot	[21]
Fake Social Network Accounts	[39]
Fake Emails	[21, 25]
Fake Websites	[13, 21]
Fake Mobile Applications / Plugin	[21, 22, 33, 40]
File Masquerading	[22, 40]
Hacking	[39]
Malware	[13, 41]
Need & greed attack	[22]
QRishing	[22]
Pharming	[33, 42]
Phishing	[2, 3, 5, 6-9, 15, 21-25, 27-41, 43-48]
Pop-up windows	[25, 29, 33, 41, 47]
Ransomware	[3, 15, 21, 33, 40, 49]
Robocalls	[33, 50]
Scareware	[9, 37, 40]
Smishing	[7, 21, 22, 24, 34, 35, 44]
Social Media	[2, 15, 48, 51]
Spamming	[21, 29].
Spear phishing	[7-9, 13, 22, 24, 25, 27-29, 33, 34, 37, 40, 48]
Spoofing Email	[39]
Trojan Horse	[24, 31, 34, 35, 39, 47]
Vishing	[7, 21, 22, 24-29, 34-37, 43, 44]
Water holing	[10, 22, 25, 29, 31, 34-36, 40, 41, 48]

We can effectively observe through the technical techniques identified above that phishing is the one that is mentioned most often in the literature, followed by baiting, spear phishing, vishing, and water holing. We found that phishing reflects its pervasive nature and significant impact on individuals, organizations, and systems. Phishing is a deceptive technique used by cybercriminals to trick users into divulging sensitive information such as usernames, passwords, and financial details by masquerading as trustworthy entities through emails, messages, or websites.

The other notable terms in the literature also represent various sophisticated forms of SE attacks designed to exploit human psychology and manipulate victims into disclosing confidential information or performing unintended actions. The prevalence of these terms in the literature underscores the evolving landscape of SE tactics and the critical need for robust cybersecurity measures and user awareness programs. We discovered that phishing is indicative of its widespread occurrence and substantial influence on people, institutions, and networks. The other techniques in the literature also refer to a variety of advanced SE attacks that take advantage of victim's vulnerabilities to trick them into divulging private information or acting inadvertently.

Contrary to the techniques that use information technologies, we can observe a list of identified non-technical SE techniques. These techniques use the victim directly to obtain confidential information (Table 7).

Table 7. SE non-technical techniques

Non-technical SE Technique	Sources
Befriending	[2]
Direct Approach	[22]
Distraction Approach	[13, 22]
Dumpster Diving	[22-25, 31, 33, 36, 43, 45, 47, 48, 52]
Hoaxing	[29, 30]
Quid pro quo	[3, 23, 27, 28, 30, 32, 33, 36-38]
Pretexting / Impersonation	[3, 8, 9, 13, 22-25, 27, 28, 30-38, 43, 5, 47, 48, 53]
Red Team	[8]
Reverse Social Engineering	[22, 23, 33-36, 47]
Role-playing	[31]
Shoulder Surfing	[22-25, 27, 28, 31, 33-37, 45, 48]
Scamming	[21]
Support Staff and Technical Expert	[29]
Tailgating ou Piggybacking	[3, 8, 24, 25, 29-38, 48, 51, 53]
Whaling	[7, 24, 33, 34, 37]

Here, we can observe that Pretexting / Impersonation, Tailgating / Piggybacking and Shoulder Surfing are the most non-technical techniques that attackers use.

These SE techniques rely less on technological sophistication and more on human manipulation and exploitation of trust and social norms. In summary, based on the SE attacks, it is possible to observe the techniques identified in the analyzed articles (Figure 9).

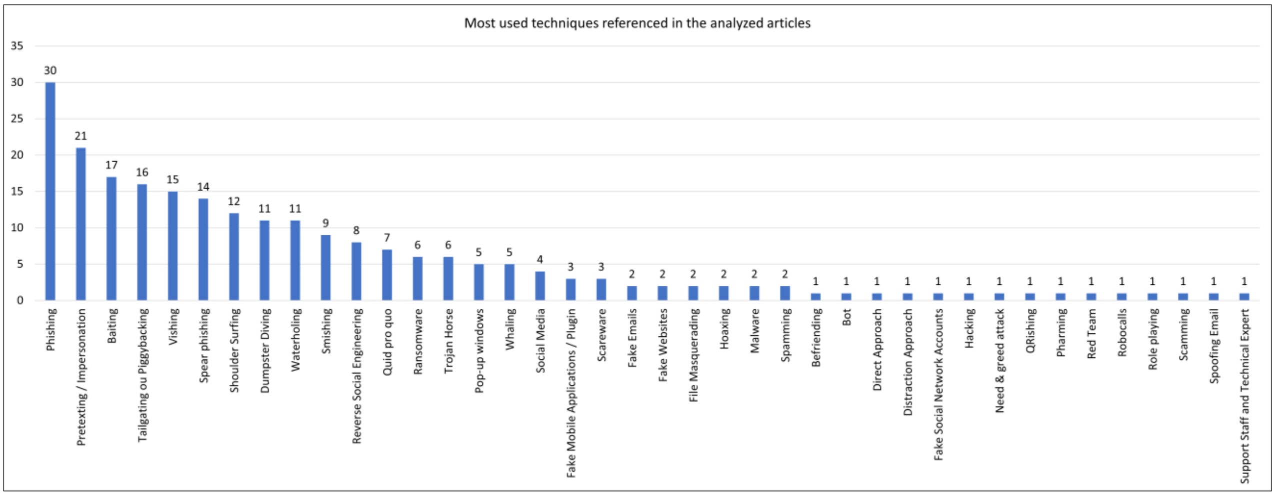

Figure 9. Most used techniques referenced in the analyzed articles

Once more, in Figure 9, phishing is the technique most often used by attackers to cheat their victims, followed by Pretexting / Impersonating, Baiting, Tailgating or Piggybacking, Vishing and Spear phishing. Other techniques are also referred to in the literature and used by the attackers. Next, we can verify the typification of the SE attack techniques, that is, which are technical characteristics, and which are non-technical (Figure. 10).

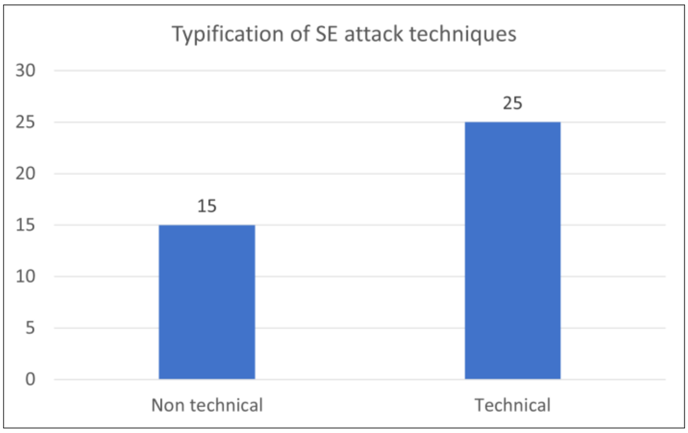

Figure 10. **Typification of SE attack techniques**

It is easy to conclude in this instance that technological attacks still outweigh non-technical threats. Investigating the ontology of SE as an interdisciplinary topic thus far necessitates social and psychological expertise, particularly regarding human vulnerabilities. This number supports our earlier assertion that increased emphasis in the literature has been placed on SE attacks utilizing more sophisticated methodologies.

To this end, a survey was conducted by Li et al. [54], and a summary of the pertinent information from previous SE investigations was provided. Persuasion factors, or human vulnerabilities, are personality features that have the potential to enhance the efficacy of seduction approaches. We can see a list of the persuasion factors that have been identified in the literature, along with a description of each. (Table 8).

Table 8. **Persuasion Factors**

Factor	Brief Description	Sources
Elicitation	One can "bring or take or come to a conclusion" with it. This method of psychological manipulation is used by social engineers to surreptitiously gather information.	[8, 55]
Persuasion	A successful relationship with the victim allows the attacker to employ a variety of persuasion techniques.	[8, 13, 55]
Authority	Having been successfully created, it is the "Holy Grail" for a social engineer because the victim receives multiple orders.	[8, 22, 31, 36, 46-48, 51, 53, 55]
Scarcity	Utilised in phishing emails that ask users to check in as soon as possible to receive cash incentives. To generate a desire of its own and then reciprocate, the target may also be drawn to seek for assistance.	[8, 22, 36, 46-48, 53]
Manipulation	To properly accomplish his objectives, a social engineer needs to master this skill. Describes manipulation as a social engineer's primary instrument; the methods of authority and scarcity discussed above fit into this category.	[8, 56]
Deception	Used by attackers to establish a sense of intimacy and compassion to win over a victim's trust. This allows the victim to feel at ease emotionally and deal with feelings like love, sympathy, affection, and friendship, among other things.	[3]
Greed	The most prevalent type of SE is characterised by messages in which the attacker attempts to take advantage of the gullible victim. "I have a large amount of money, and I promise to give you half if you offer me any information about you."	[31]
Fear	The victim may act abnormally due to fear inflicted by the attacker. Here, the attacker takes use of the victim's fear to blackmail him by claiming to be in possession of crucial information about him. If the victim does not pay the demanded amount, the information will be made available to the public on the Internet. One of the key elements that social engineers exploit is fear of the unknown. For instance, the social engineer establishes himself as the boss and demands that certain tasks be completed. The victim will now consider what could go wrong because she is afraid of what can happen.	[22, 31, 47, 51, 53]
The feeling of urgency	The attacker persuades the victim of a lucrative offer (often through marketing campaigns).	[31]
Curiosity	Several articles, pictures, and videos pique people's curiosity by using terms and phrases like "shocking," "will not believe," "sensational," and similar ones to entice viewers to click on the content. Curiosity therefore forces people to respond in ways that they might not otherwise.	[22, 31]
Sympathy	By using deception techniques, the attackers manipulate the victim's emotions by fabricating stories about sensitive or unpleasant subjects, such as "We were attacked in the hotel where we were," to extract money, which the criminals then demand but never deliver.	[31]
Respect towards authorities	The victims believe that they are speaking with a manager, a supervisor, or another employee of their place of employment. However, the PCs would have been infected with ransomware if the intended victim had clicked on any of the links.	[31]
Trust in a certain person	Messages that seem to be from mentors, instructors, and other reliable individuals are given to victims. These messages may contain links that are harmful or malicious. Even if a link seems to have been supplied by someone you can trust, you should still carefully examine it before clicking on it.	[31]
Liking and similarity	People who they relate to or find appealing can easily win people over. This human element is used by social organizations to influence people to take the required actions.	[22, 47, 48]

Social Proof	Individuals act based on how those in their immediate vicinity behave. This social proof element is poorly used by social engineers to accomplish their objectives.	[22, 36, 46, 47]
Commitment	People are more likely to follow through on a promise if they acknowledge the desire or aim. People believe their perception of themselves will suffer if this desire or objective is not achieved.	[22, 47, 48]
Reciprocation	People usually repay favours. A social engineer will manipulate this type of human factor when they require important information.	[22, 36, 47, 48]
Human need and greed	Humans are susceptible to their own desires and avarice. Social engineers take great care to understand your wants, desires, and greed in order to exploit that knowledge to further their objectives.	[22]
Friendship	People typically comply with a friend's or relative's request for a particular deed or favour. This element is used by social engineers to gather data or accomplish goals.	[22]
Distraction	The social engineer can obtain as much information as he wants while the victim is preoccupied. For instance, to get the victim out of a room, get a glass of water.	[13, 22]
Deceptive principle	People are generally not what they display. This is a common tactic used by social engineers, who may easily trick the victim into believing what they are saying.	[22]
Trust	Individuals frequently depend on others, and the attacker takes advantage of this tendency towards trust. In order to get information, the social engineer first builds victim confidence and coerces them into doing desired activities.	[22]
Time pressure/urgency	A person under time pressure makes decisions in a different way. Social engineers employ this element to put the victim under time pressure and prevent them from considering reasoning since there is less time for thought and they are expected to react swiftly.	[22; 53]
Diffusion of responsibility	When others are involved, a person is less inclined to assume accountability for the work that needs to be done.	[22; 47]
Laziness	If someone can do a particular work but chooses not to do it because it requires effort, that person is deemed lazy.	[22]
Natural inclination to help	People are naturally inclined to lend a hand to those in need.	[22]

Through the previous table (Table 8), the referred SE techniques, defined as human vulnerabilities, could be used by attackers to obtain confidential information from the victim without using technological methods or tools.

We discovered that some of the most well-known non-technical techniques that attackers employ to directly exploit the weaknesses of their victims are Authority, Scarcity, Persuasion, Fear, and Social Proof. These psychological ideas prey on people's decisions and behaviors to deceive them into divulging personal information, acting in a particular way, or complying with evil requests. Subsequently, we shall analyze the subsequent research inquiry concerning the elements that contribute to the effectiveness of SE attacks.

5-2- RQ.2: What Factors Contribute to the Success of SE Attacks?

According to experts, cybersecurity inertia actively plays a role in successful cyberattacks that pilfer private personal information and sensitive data from organizations. These attacks can affect election processes, harm businesses, and result in identity theft [23]. Insufficient training and user awareness have been found to be the primary causes of the majority of successful SE attacks [44].

As has been analyzed, people are easily misled and have many vulnerabilities, which makes many SE attacks successful. There is a serious risk to data confidentiality when user data acquired through security breaches is routinely leaked [25]. The primary human behavioral traits that contribute to the success of SE attacks are described as follows [57–59], cited by PÎRNĂU et al. [31]. So, the success factors for the SE attacks could be observed (Table 9).

Table 9. Success Factors

Success Factors	Sources
The joy of victory – the victim receives an email from the attacker that makes her feel happy and encourages her to download malicious software.	[31, 57-59]
Fear of Authority – because so many people find the authorities intimidating, attackers take advantage of this psychological weakness to steal confidential information.	[31, 57-59]
The desire to be useful – attackers get a lot of data by posing as somebody who can be helpful to the victim; this material is typically kept private from outsiders. The attacker can access the target machine thanks to all this info.	[31, 57-59]
Fear of Loss – the attacker emails the victim and claims to have made a lot of money, but just needs to transfer a little sum into a certain bank account. The victim realises it's a fraud after depositing the money into the designated bank account out of fear of losing such a chance.	[31, 57-59]
Insufficient knowledge – the victims' lack of awareness is the foundation of this kind of attack. Social engineers take advantage of this weakness by instilling a sense of urgency, depriving the victim of time to think things through and making them the target of an attack.	[31, 57-59]
User accommodations with reference to the implementation of policies and best practices for Information Security.	[2]
Some employees are resistant to and uninterested in using social networks in favour of conventional procedures. This may lead to instances of noncompliance and misinterpretation of security-related matters.	[2]
Organizations are becoming more and more interconnected on a global scale, encompassing multiple cultures and regional norms with varying degrees of vulnerability to threats.	[2]

Cloud storage, security, and payment service providers are examples of businesses that outsource business processes and have their own Information Security rules and procedures for staff members and systems.	[2]
Conventional business models like "command and control" operate with the modern, adaptable, and nimble models required for societal acceptance.	[2]
There are gaps in the current Information Security policies that make it difficult to address social network use and the unique risks that come with it, such social engineering.	[2]
Social engineering (SE) via social networks is one of the new risks that traditional firewall-protected networks cannot effectively counter.	[2]
Organizations' information assets are at risk due to the growing prevalence of "BYOD" policies and unprotected social media usage on both a personal and professional level.	[2]
Employees typically use the same username and password across various social, personal, and professional accounts.	[2]
In the context of social networks, organizations lack direction or have a vague plan in place for handling SE attacks or Information Security incidents. This leads to liability, harm to the organization's reputation, and loss of financial resources, among other consequences.	[2]

We referred to SE success factors (Table 9) that help attackers achieve their objectives. Organizations and their staff typically lack the expertise required in this context of Information Security, and they are not prepared to handle these issues. Success variables play a critical role in determining the efficacy of manipulative techniques employed by attackers to exploit human vulnerabilities and achieve their objectives. Among the many other critical success variables discussed in the literature, four stand out as crucial: the thrill of victory, the fear of failure, the fear of authority, and the lack of knowledge. Training and knowledge aid in preventing these kinds of success factors. We will learn about the barriers known as SE attacks through the following questions:

5-3- RQ.3: What Obstacles are Referred to in the SE Attacks?

The way businesses and organizations handle SE attacks should be included in their risk management plan because they provide serious security threats [60], cited by Salahdine & Kaabouch [33]. Businesses need to make a commitment to fostering a safety-aware culture among their employees.

Several techniques have been proposed to detect, prevent, and mitigate these attacks. These include promoting security education and training, raising social awareness of the SE, giving the tools necessary to detect and prevent these attacks, teaching new hires how to protect confidential information, organizing security guidelines, informing employees about the risks of advertising attacks, and forwarding emails that are known to be fraudulent, as well as sensitization emails [61], cited by Salahdine & Kaabouch [33].

SE targets both private citizens and even the most sophisticated and safe institutions. The goal of defense tactics and preventative measures is to shield them against SE attacks. These manual and automated methods are perhaps the bare minimum that a business or organization needs to protect itself from the most frequent SE attacks. Mechanisms can be established in one or several organizations.

Artificial intelligence-based defense measures are the most successful ways to lower the likelihood of SE attacks, according to an analysis and comparison of different strategies. Furthermore, enhanced protection may be obtained by combining two or more defensive strategies. The degree of readiness dictates the capacity to avert, identify, lessen, and confine any questionable behavior [33].

One can categorize prevention approaches for SE attacks as predictive, remedial, or preventative. As of right now, hiring and employment practices, process creation, technical controls, education, training, detailed defense, and security policy development have all been recognized as preventative measures against SE attacks.

These measures can be seen primarily as preventive measures and, therefore, occur before a potential attack [62]. Based on Abeywardana et al. [8], the authors suggest three topics for discussion in SE workshops at the organizational level:

- Acquire the ability to recognize SE attacks: each employee needs to have a basic awareness of both SE and its attack vectors. Employees should learn about phishing emails, dangerous attachments, and how to spot shady letters from workshops.
- Raise awareness of personal safety: Employees should pay attention to their personal area. Most security mishaps can be avoided if an employee feels comfortable using their desktop, laptop, and smartphone and is aware of the need to maintain the devices' integrity.
- Information value and action magnitude: Every employee needs to be aware of the organization's assets and the significance of the information available for request. It is always necessary to ask yourself, "Do I need to reveal this information?" The tasks that employees must complete can be handled using the same logic. Managers within the organization need to have a process in place for handling these kinds of situations so that workers may easily contact a higher-ranking official when needed.

Even though preventing SE attacks is vital for nations and organizations, research lacks on defense measures against the several SE attack vectors. In this way, a taxonomy is offered to aid in the understanding of SE attack defense systems by professionals, researchers, and organizations. Employers can utilize taxonomy to better safeguard their data by educating their staff about the several defenses available to them [25]. Based on the research conducted by Alharthi & Regan [25], it was determined that social engineers should focus on five key areas, which include the primary resources of every organization. People, Data, Software, Hardware (SW/HW), and Network are these five key components.

In this regard, organizations need to spend money on employee education and awareness campaigns about this kind of attack [51]. According to the same perspective, the report [63] also mentions training solutions and the most recent methods that organizations are using to reduce any risks to the SE, such as gamification, serious games, tournaments, virtual labs, and the usage of other contemporary apps. Like this, there are now conferences, thematic training, video streaming, awareness campaigns, and awareness campaigns that teach people about SE risks.

According to the literature study done by Aldawood & Skinner [45], the following Information Security training techniques have room for improvement: accessibility to online learning materials, such as email, social media advertising, synchronous and asynchronous discussion, blogging, and animation; games that can engage, inspire, and test the members of an organization (gamification); videos that let viewers study individually and at their own speed; To gauge employees' awareness and susceptibility, phishing emails are included in the simulation.

Resistance training methods equip workers to defend themselves in the case of a SE attack. Programs to raise awareness for people or organizations that have been specifically designated as the main objectives of a SE initiative are included in this context. Because hackers constantly refine and adapt their attacks to circumvent various security measures, it's critical to regularly implement these awareness campaigns to keep people informed about new advancements. An essential part of educating people about SE assaults is demonstrating how susceptible they are and how to recognize an attack victim [3].

Organizations' defenses against attacks can be strengthened with proper standard awareness and training. To make sure that any new subjects are covered, and the previously covered ones are brought back, this training should be conducted often [37].

For instance, training needs to be done to make sure that every employee is aware of the various strategies that attackers use to take advantage of a victim. Another workable option is to stress the need to safeguard the organization's overall privacy to stop any personal data from being leaked and make it easier for an attacker to access it. Employee training is, in practice, the most successful mitigating method for SE. Organizations can effectively turn their weakest link into their strongest with regular reminders that stress the need to remain watchful against suspicious behaviors as well as periodic and systematic security training.

Employees need to be aware of the significance of safeguarding confidential data and the methods that a social engineer may use to conduct an attack. With increased awareness, they can learn about multiple attack avenues and become proficient at telling the difference between a direct strike and one that is more general [64]. In their study, the authors list a few strategies to enhance the way in which staff members are trained about SE attacks: onsite training, intranet-based teaching materials, screensavers, posters, reminders, and online courses.

Certain organizations can detect and stop SE attack attempts by providing training to their staff. It is far simpler to train staff members on SE principles than it is to shape them into technological systems like firewalls. With the right preventive measures in place, people will no longer be the weakest link in the security chain and instead act as a shield to safeguard the organization [45].

To identify gaps in users' capacity to recognize and stop SE attacks, it is crucial to examine user behavior and perceptions of these attacks.

Additionally, Esparza et al. [15] mention the idea of "cyber hygiene," which is characterized as a set of cybersecurity precautions that internet users must take to safeguard the security and integrity of their personal data and any equipment that might be the target of an online cyberattack [65]. Since cybersecurity inertia can only be eliminated if all company stakeholders participate in its mitigation, several variables are listed in Table 6 by Borkovich & Skovira [23] and are advised for application throughout the organization regarding the reduction of SE risks (Table 10).

Table 10. SE risk mitigation factors

Factor Description
Include cybersecurity and SE missions in the ethics and code of conduct for staff members.
Provide and conduct regular safety awareness and training sessions for all staff members; mandate that each participant sign a certificate of recognition upon completion of the course.
Create a policy for the classification of data and information, and share basic settings for classified, proprietary, sensitive, and other categories.
Establish guidelines for establishing an applicant's identification and the "need to know" explanation with managers or supervisors.
Provide employee education initiatives that focus on recognising and fending off SE threats.
Test staff members' ability to withstand SE attacks on a regular basis by modelling scenarios with anonymous attackers.
Conduct numerous exercises and safety and SE compliance audits every six months; notify all staff members of the test results.
Arrange for regular evaluations, audits, and meetings with facilities, vendors of cloud storage, and suppliers.
Adjust the security culture within the organization with more knowledge, tact, and healthy scepticism.
Motivate staff members to embrace and use security protocols by offering incentives like as awards, certificates, gift cards, bonuses, team competitions, lunches, and/or snacks.
Include cybersecurity accomplishments and SE awareness as evaluation factors in yearly performance appraisals.
Posters, screensavers, and advertisements for security policies should be sent by email, videos, and newsletters.
At meetings, ask professionals in behavior and security concerns to speak as guests.
Establish a "Champion" of SE and make sure senior management is on board and financially committed.

As we can see, implementing these elements could assist companies in reducing SE risks and serve as best practices to minimize this issue. This calls for a diversified approach that considers both technological weaknesses and human variables. It is necessary to teach staff members and users about common social engineering tricks, red flags, and recommended practices to foster a culture of security awareness. By integrating these mitigating variables, organizations can successfully reduce their exposure to SE assaults and increase their overall resistance to evolving cybersecurity threats. Additionally, some authors discuss methods for eradicating cybersecurity inertia in businesses (Table 11).

Table 11. SE risk mitigation plan – strategies to eliminate cybersecurity inertia

Obstacles	Sources
Employee education and awareness regarding the avoidance of SE attacks.	[2, 6, 52, 66]
Managers' awareness of organizational Information Security.	[2]
Refuse requests for passwords or sensitive financial information.	[3]
Reject offers or pleas for assistance from dubious organizations.	[3]
Configuring 'high' spam filter settings in email applications.	[3]
Check the spam folder occasionally to check if any emails there are authentic.	[3]
Installing and making sure that firewalls, email filters, and antivirus software are updated. Malware employed by attackers has the potential to affect Information Security software. As a result, the software developers who create these apps keep an eye on these behaviors and take these risks into consideration when they upgrade their programmes and add new algorithms and updates. Because of this, users should oversee updating their software to the most recent versions to prevent the usage of hacked versions, which could alter the information's integrity.	[3]
Typically, spammers want their victim to act without thinking first. The user should pay close attention and carefully consider the request if the notification indicates that a response is required immediately.	[3]
Take care when downloading anything. It can be a mistake to download anything from an untrusted source if the sender is unknown or questionable.	[3]
Security policy: Executive management should incorporate both technical and non-technical employee-focused techniques into a well-written policy. Security must be integrated into every organization's operating goals.	[32, 45]
Network guidance: The company needs to employ network address translation (NAT), put approved websites on the allow list, disable unwanted apps, and secure the network. Users of the network must create complicated passwords that are updated every sixty days.	[33]
Audits and Compliance: Organizations need to make sure that their security guidelines are being actively followed. Examining network logs, confirming employee permissions, and checking desktop configurations at least every two months are a few detection controls.	[32]
Technical procedures: To safeguard data and the main infrastructure, the network needs to have several levels of defense. All devices need to have software installed, such as firewalls, intrusion detection systems, and intrusion prevention systems (IPS and IDS). All external services need to have web filters, virtual private networks (VPNs), and demilitarised zones (DMZs) implemented.	[32]
Physical Orientation: A variety of measures can be taken to safeguard tangible goods. It is advantageous to use a variety of security tools, such security cameras, to keep attackers out of the building. Organizations must utilise biometrics, access control lists, or multi-factor authentication before granting access in places where physical hardware is situated.	[32]
Emphasises the protection of individual privacy.	[45]

Therefore, one of the easiest yet most efficient ways to defend the end user against SE attack vectors is through ultimate user awareness [67].

Due to their multidisciplinary nature, SE attacks are increasingly damaging large-scale sociotechnical systems; nonetheless, relatively little research has been done to assess security requirements. According to the authors, one of the most important issues is determining the likelihood of SE assaults with accuracy and efficiency, since without it, risk analyses cannot be carried out and the necessary security standards cannot be met [12]. Knowing the models or frameworks that have been in place for the past two years that could aid in preventing SE attacks is crucial in this situation.

5-4- RQ.4: What Are the Existing Frameworks or Models for Preventing SE Attacks in the Last Two Years?

During this investigation, several SE models/frameworks were found in the literature. In this sense, a summary of each identified artifact is presented (Table 12).

Table 12. Frameworks and models comparison

Author	Framework / Model	Year	Description	Areas	Advantages	Limitations
[9]	Model for security threats and attack methods.	2021	Proposal of a basis for the development of security techniques.	Attack Defense Attack Methods Consequences	Covers security inside and outside the system to prevent SE-based attacks.	Limited to attack prevention with phone calls. Only for test proposes.
[10]	User-centric framework.	2018	Framework for assessing and understanding employees' perspectives when using social networks to initiate more effective education-based interventions.	Attack User characteristics that can influence user analysis of online attacks	Selected attributes for the user-centric framework were categorized and grouped into themes relative to the nature of the attribute. Easy to understand.	Only focused on education-based interventions. It can be proposed to raise people's awareness and skills to detect threats on social networks.
[3]	User-centric framework - threat detection capability factors.	2019	Realise and build a coherent understanding of user vulnerability to social engineering attacks in the information security context.	Attack User vulnerabilities	Understanding of the main vulnerabilities of the users.	Only an overview of user-centric characteristics that may affect the user's threat detection capability factors may influence the user's judgement on SE. Attacks.
[5]	Social Engineering Attack Detection Model (SEADM).	2017	Provides a general procedural template for implementing detection mechanisms for SE attacks.	Defense Training	To help people identify malicious SE attacks.	No states to examine the emotional state of the user. Not tested with real subjects.
[11]	User-Based Security Training Model (STRIM).	2020	It aims to educate and train users to detect, avoid, and report cyberattacks in which they are the primary target.	Defense Training	Employees are aware and up to date and can understand, detect, and report cyber threats. Include a novel approach and strategies for effective learning, training, and awareness as a key part of developing security. It could help organizations establish security-conscious behaviors among their employees.	It cannot solve all the security threats at once. For example, Zero-day exploits and social engineering scenarios are unpredictable, and it is not easy to defend against them.
[12]	SE attack analysis framework.	2019	Analysis approach for dealing with social engineering attacks.	Attack	Assess the probability of SE attacks by automatically checking the SE attack scenarios in the repository.	Due to the inherent uncertainty of the SE attack, it is hard to determine whether the assessment results are correct.
[13]	Social Engineering Scenario Analysis Framework.	2021	Use the analysis of the social role and a theory-based approach to interpret even more the scenarios of the SE.	Attack Training	Acquire knowledge about existing SE scenarios, social roles, vulnerabilities of the victims, principles exploited by attackers and respective storylines.	Some of the scenarios taken from sources may be fictionalized to some extent. A limited number of scenarios can be cross verified by adding more SE scenarios. It was only focused on the successful scenarios from the attacker's perspective.
[68]	Internal threat risk prediction framework.	2018	It helps organizations and can predict potential malicious threats before an SE attack.	Defense	Based on a multiple-approach perspective. Integrated with key internal threat indicators. It is possible to predict who may be an internal threat based on the calculation of three dimensions: a) Technological aspect. b) Organizational Impact. c) Human Factor.	No single approach can eliminate this kind of security breach. Organizations need to carry out a regular security risk assessment regarding insider threats.
[15]	Framework for cyber hygiene modeling	2020	Includes human factors in the design of self-assessment and modelling tools, accurately, of the aspects related to cyber hygiene that are the root cause of cybersecurity problems.	Defense Risk	The categorization of risk dimensions in their atomic components improves the evaluation of the effectiveness of the intervention in the context of cyber hygiene.	Only related to human factors.

Through the previous table (Table 12), a brief analysis of the most relevant SE models/frameworks found during this SLR was carried out. The name, year of publication, a brief description, area of intervention, advantages, and limitations were identified. In terms of scope, it can be stated that the areas covered are mainly related to attacks or attack methods. These user characteristics can influence the user's analysis of online attacks, consequences, user vulnerabilities, defense, training, and risk. In this sense, the next section aims to present the results of this investigation.

6- Discussion of the Results

It is verifiable that most organizations depend on Information Security. Potential SE threats have increased in recent years, increasingly use new techniques and greater sophistication, and are more difficult to detect. In technical terms, it was possible to observe that of the numerous techniques mentioned in the literature, the most imminent threat to which organizations are exposed is undoubtedly phishing, and the exploitation of human vulnerabilities is a growing threat of SE when the attack is not carried out directly through technical means. Since attackers can succeed by collecting the needed information by taking advantage of human vulnerabilities, present defensive methods do not appear to be sufficient for mitigating the sophistication of SE attacks. Determining an organizational plan to raise employee understanding of the issue and sensitise them to it is therefore important to lessen the ignorance of Information Security.

Information security hazards are without a doubt the most difficult for an organization to manage [53]. To reduce these risks, a lot of organizations often use technology-based solutions. While important, these are frequently insufficient to address all possible dangers. It was evident that a crucial component of Information Security is the human aspect. This necessitates managing related risks, such as SE attacks. Organizations are facing growing difficulties in Information Security because of various threat scenarios. To reduce the risks associated with the potential of SE attacks, it is vital to implement frameworks that can direct staff members towards the adoption of best practices in the context of Information Security.

Bring Your Own Device (BYOD) policies allow employees to use personal devices on company networks, particularly for social network access, raising concerns about Information Security within the organization. The expansion of this strategy in recent years raises the possibility of Information Security lapses within the organization, which could result in data loss and altered information integrity and cause major disruptions to the operations of the organization. People post all types of information on social media without thinking that it could be exploited by someone who wants to undermine the security of the organization they work for Duarte et al. [51].

In this sense, there is no doubt that organizations should think about their security policy, developing and updating it frequently to communicate it at all organizational levels based on good Information Security practices. Regarding organizational controls and best practices for staff members in relation to SE threats via social networks, a gap in the literature has been noted in this area [2]. The authors propose a framework, dubbed SESM (Social Engineering through Social Media), to address this problem. It conceptualizes organizational implementation by relating pertinent IT security standards to the creation of security guidelines for social network use and SE mitigation.

Preventive approaches are ineffective in addressing the growing number of SE attacks, and existing detection technologies have basic limitations. Subjective decision-making is a limitation of human-based systems. Because technology weaknesses can be exploited, technology-based techniques might also have limitations. Attackers are getting stronger and more intelligent every day, and these attacks are changing regularly. Therefore, to identify and lessen the effects of these attacks, there is a critical need for more effective detection and preventive approaches. Employee training programs should be developed since people pose a threat to a network's security [33].

Information Security awareness-building and training initiatives enable all staff members in a company to get safety-related information. ICT users who are aware of Information Security are more empowered and can respond appropriately to possible threats to Information Security [69]. Information Security is respected in organizational settings, and security workshops are frequently held there. It is deemed necessary to equip workers with the knowledge they need to defend themselves from attacks, even when these workshops don't cover subjects like SE, which are frequently disregarded [8]. Furthermore, it is important to periodically reinforce these workshops because, after training, individuals could forget and revert to their previous behaviors. In terms of preventing SE attacks, these programs are essential tools that help participants get ready for the future as well as the present [28].

The research indicates that, before introducing new technical protection solutions, training and awareness campaigns should be considered. This aids in preparing the company and its staff to defend against threats and tactics used by social engineers [63]. Attackers choose which asset or victim to target, when to attack it, and under what circumstances. People need to be made aware of SE attacks and the risks associated with excessive information sharing online in the digital age, when nearly everyone is linked via a mobile device [22]. The Information Security community should be inspired to enhance current training programs and create efficient countermeasures against the risks of SE attacks, specifically those carried out through the phishing technique, as per the conclusions drawn by the study of Alyahya & Weir [46] on SE attacks conducted through that method. But according to Washo [70], SE research has to be strengthened from an ethical standpoint. It can be confirmed that staff training in organizations becomes highly relevant to raising the bar for knowledge and reducing SE attacks. But to do this, simulated attacks must be conducted, which brings up the ethical considerations in SE. System administrators may find it challenging to persuade users of the urgent need for these tests since some users may view the ethical hacking component as a privacy invasion. This presents a new challenge to training. The application of multiple SE approaches and success variables is involved. It is challenging to stop every possible attack since nothing is 100% safe, even with the best security systems in place.

To make the frameworks and models under analysis better, other elements can also be investigated. Following the preceding investigation, we discovered several gaps in the literature, which had an impact on the proposed SE frameworks and models. From a non-technological perspective, there is a deficiency of knowledge on SE attacks.

Through the following critical analysis, the following SE prevention frameworks will be explored, analyzing their contributions, challenges, and practical implications. The Model for Security Threats and Attack Methods [9] presents a proposal of a basis for the development of security techniques. It covers security inside and outside the system to prevent SE-based attacks but is limited to some types of attacks and vulnerabilities. Based on the analysis of the secondary data sources, several key elements of SE attacks have been recognized: Humans, Psychological and Emotional Exploits, Technology, Security Awareness, and Types of Attacks.

This conceptual model shows the various aspects, namely four: Vulnerabilities, Defenses, Attack Methods, and Consequences. Based on these, almost all SE attack's sources can be stemmed out. In practice, it proposes an expanded way to deal with building up a security technique by embracing security inside and out of the system to avoid SE-based attacks. There is an exploration impediment that must be examined here. The framework primarily focuses on IT-related aspects of SE attacks, such as technology, security awareness, and types of attacks.

Subsequently, the authors used the combination of several security algorithms as a methodology to develop a new hybrid security model. In the context of cryptographic algorithms, various types of SE techniques, attackers' behavior, prevention measures, damage to Information Security and how to perform a recovery after potential attacks are analyzed.

It's a very interesting framework; however, it lacks a broader perspective that includes non-IT factors such as organizational culture, human behavior, and social dynamics, so it may lack depth in analyzing the underlying psychological and emotional factors driving such attacks. Different organizations may have unique vulnerabilities, defenses, and attack methods. For developing comprehensive defense strategies, it is crucial to know how this can intersect with these non-IT aspects. Also, only generic exploits and countermeasures are available for organizations.

A framework for assessing and understanding employees’ perspectives when using social networks to initiate more effective education-based interventions was developed by Albladi & Weir [10]. It is a framework developed in the context of SE attacks, namely user characteristics that can influence user analysis of online attacks, more specifically, on social networks. It turns out to be one of the very important issues in the context of the SE, but it is the only focus. Although it does not provide clear guidance on how these characteristics are related to vulnerability to SE attacks or how they can be minimized.

Without actionable insights on mitigation strategies, organizations may struggle to effectively address SE risks. A multidisciplinary approach could provide a more comprehensive understanding of SE vulnerabilities and inform targeted intervention strategies. In any case, it is a framework that can be used to complement other models and even training sessions and prevention strategies in organizations, improving the behavior of the most vulnerable employees through a new level of security.

The framework presented above by Albladi & Weir [10] could be complemented by the user-centric framework—threat detection capability factors [3] and vice versa. It allows for a perception of human vulnerabilities by presenting four types of variables: psychological, perceptual, habitual, and emotional. A proposal for a defense cycle for SE attacks is presented, as well as some generic recommendations for prevention. In this model, the importance of psychological aspects, emotions, and human vulnerabilities is highlighted. It helps to have an overview of factors that may influence the user's judgment on SE, but in any case, it would be important to present effective prevention measures for these aspects.

While this is an important aspect, it may not address other critical factors that contribute to SE vulnerabilities, such as organizational culture, technology infrastructure, and the external threat landscape. Effective prevention strategies require more than just understanding vulnerabilities. The framework could include practical steps that organizations and individuals can take to mitigate risks and strengthen their defenses against SE attacks. Also, in SE attack detection, Mouton et al. [5] developed the Finite State Machine for the Social Engineering Attack Detection Model, which provides a more detailed view of the implementation of mechanisms for detecting SE attacks compared to the previously developed models, which were populated with questions related to SE attacks that use various types of communication (unidirectional, bidirectional, or indirect).

This model makes use of a decision tree and breaks down the process into more manageable components to aid decision-making. It's extensible, and even if it doesn't respond to all types of attacks, it's already a step forward in the SE research field, helping to think differently about SE attacks. For example, considering previous models, in terms of vulnerabilities, this model does not have states to examine the user's emotional states, which are important indicators of susceptibility to SE attacks.

Emotional manipulation is a common tactic used by attackers to exploit vulnerabilities and coerce humans into revealing sensitive information or performing actions against their better judgment. Incorporating mechanisms to assess and analyze users’ emotional states could enhance the model’s ability to detect and mitigate SE threats. Also, it may have limitations in handling complex attack scenarios and variations.

A Critical Thinking Model for Security and Privacy was introduced by Hamoud and Aïmeur [11]. This model introduces a theoretical user-based security training model called Security Training Model (STRIM), which aims to educate and train users to detect, avoid, and report cyberattacks in which they are the primary target. The proposed model by the authors could be a solution to help organizations establish security-conscious behaviors among their employees.

It is a model that aims to satisfy cybersecurity requirements by creating user awareness of content that focuses on various new and emerging threats. STRIM incorporates non-technical aspects such as manipulation, cognitive bias, and security behavior. Every user is trained to detect and avoid different kinds of cyber-attacks, and their progress and vulnerabilities are tested by an ethical hacker who tests user responses to a cyber-attack. Ethical hacking tests may not always replicate real-world attack scenarios accurately, and users may respond differently in actual attack situations compared to controlled testing environments.

Additionally, the ethical hacker's expertise and resources may be limited, leading to gaps in the coverage of potential attack vectors and techniques. This model focuses on developing a sense of skepticism and rationality among users by inviting them to refuse or accept digital interactions without thinking about the consequences. However, this proposed solution cannot solve all the security threats at once.

For example, this model may not adequately address the challenges posed by zero-day exploits and sophisticated SE scenarios. It emphasizes developing security-conscious behaviors among users, but it may not provide sufficient technical training to empower users to recognize and respond to SE threats effectively. Understanding the technical aspects of common attack vectors, such as phishing emails, malware, and network vulnerabilities, is essential for effective SE threat detection and mitigation. This type of model requires continuous reinforcement, ongoing evaluation, improvement, personalized feedback, and incentives to sustain user awareness and vigilance against evolving SE threats.

An SE Attack Analysis Framework has been outlined by Li et al. [12], which consists of a general process for analyzing SE attacks. They summarize a list of challenges that become the bottleneck of SE research. On one hand, given the list of challenges, they admit the difficulty of investigating SE attacks. On the other hand, they believe that their preliminary proposal is useful and beneficial for subsequent research on SE.

There is no efficient security requirements analysis approach for dealing with SE attacks. One major obstacle to this problem is the uncertainty of human behavior, making it difficult to effectively assess SE attacks. Security requirements analysis is essential for understanding the security needs and vulnerabilities of systems and organizations.

Integrating security requirements analysis methodologies with SE attack analysis could help identify gaps in security defenses and inform the development of effective countermeasures. Addressing these gaps could help strengthen the framework for analyzing SE attacks and enhance its practical utility in research and practice.

Another alternative for an SE Attack Analysis Framework is proposed by Yasin et al. [13]. It analyzes the existing SE scenarios in terms of the social roles played by victims and attackers, the underneath vulnerabilities of the victims, the principles exploited by attackers, and the storylines composed by the attackers. Although there is a need to investigate those cases where the attacker was unsuccessful in achieving the desired goal and extract the reasons why that attack remains unsuccessful. Understanding unsuccessful attacks and the reasons behind their failure can provide valuable insights into the effectiveness of defense mechanisms, user resilience, and potential vulnerabilities that were not exploited, helping identify areas for improvement in security measures and user awareness training.

A prediction framework is presented by Aldawood & Skinner [14] that will assist decision-makers in eliminating cyber security insider threats. This helps organizations predict potential malicious insider threats before a breach takes place. The emergency insider threat risk prediction framework is based on a multiple perspective approach integrated with Key Insider Threat Indicators; through this framework, the authors predict who could be an insider threat based on the three-dimensions calculation: a) Technology Aspect, b) Organizational Impact, and c) Human Factor.

While this framework incorporates key insider threat indicators, it may not cover the full spectrum of indicators that could signal potential SE insider threats. Insider threats can manifest through various behaviors, actions, and patterns, including unauthorized access to sensitive information, changes in behavior or work patterns, and attempts to bypass security controls. The framework may need to be expanded to encompass a broader range of indicators to enhance detection accuracy and effectiveness.

In terms of human vulnerabilities, a framework for cyber hygiene (CH) modeling was developed by Esparza et al. [15]. This includes human factors in the design of self-assessment tools for accurately modeling CH aspects that are the root cause of CS issues. Furthermore, categorizing risk dimensions into their atomic components is expected to enhance evaluating the effectiveness of CH interventions.

The authors aim at enhancing the design of self-assessment tools so that organizations can create better questionnaires that achieve a more in-depth picture of the respondent and enable identifying the types of threats together with their root causes. CH helps strengthen people's resilience against SE attacks through safe online practices and behaviors, such as recognizing suspicious activities, updating systems and devices, making conscientious use of social networks, verifying the authenticity of the sources used, and constantly learning and adapting to the latest attack techniques.

At this point, SE prevention frameworks were presented, analyzed, and discussed, considering their area of application, advantages, and limitations. These frameworks offer distinct approaches and varied strategies to address the challenges posed by SE. By evaluating these frameworks, it is possible to identify strengths, limitations, and opportunities for improvement in defending against SE attacks. By better understanding the different approaches and perspectives offered by these frameworks, it is possible to guide efforts to strengthen organizational resilience against the threats posed by SE.

By the end of this discussion, it is intended to provide a broader understanding of SE prevention frameworks and stimulate reflections on best practices, innovations, and ongoing challenges in defending against these threats. Most SE frameworks/models present in the literature are focused on attack techniques and methods, that is, mostly on technical components, in multiple online applications, namely in social networks, decorating defense mechanisms related to the human factor.

Humans are frequently the weakest link in the chain of Information Security, thus, technology by itself is rarely a sufficient defense against information theft. The attackers' creativity is the only thing limiting the user's awareness, the subject's breadth, and the range of potential outcomes, demonstrating that even individuals who are aware of a SE attack, for example, phishing, are vulnerable to one. SE techniques are a staple of most effective information system attacks, and they always will be as long as people have all of their natural instincts and emotions [71].

Human user prevention systems include cybersecurity awareness campaigns, training, and organizational policy and process implementation. One of the best ways to guard against being the target of SE attempts is to train staff members on the many kinds of these attacks. Information Security in organizations must be protected with awareness of and resistance to SE threats. Additionally, it's critical to consider the requirement for a multidisciplinary strategy that involves features that are educational, behavioral, and technical. Organizations should make a constant effort to raise awareness of SE attacks and incorporate them into their everyday operations [52].

Because technological approaches do not fully account for the behavioral, cognitive, and heterogeneous motivations that lead to human error in the security causal chain of Information Security using SE methods, the current technical and intelligent defense mechanisms can only partially increase the resilience of IT systems. Incorporating human elements into the security chain is crucial, as it aids in the detection and prevention of issues. It should instead be viewed as the strongest link in Information Security in this situation, not a weak one [72]. Human error is now the main factor that makes SE attacks viable. Many employees and users lack the necessary training or understanding of the various kinds of SE attacks. As a result, SE has been used by hackers against them. It is imperative to acquire knowledge about cyber risks and strategies to avert them, such as adopting technological tools and resources or adopting a different perspective when confronted with a purported SE attack [38].

Cybersecurity is a shared responsibility, and every employee of an organization is vital to its cyber protection and countermeasure efficiency. Because of this, every employee needs to be informed on organizational rules and procedures that are pertinent to their job function and be aware of any potential hazards in their field of work. They should also be able to identify questionable cyber activity, report it, and, if feasible, take action to stop it. An organization can lessen its vulnerability to human error-related cyberattacks and avoid unintentional data leaks by increasing the cybersecurity awareness of its workforce [73].

It should also be noted that there is a lack of artifacts that allow organizations to increase control over the behavior of their employees concerning the use and communications they can establish, either online or with other individuals, potential attackers. It would be useful to provide organizations with a set of tools that would make it possible to make their employees aware of SE's problems, which are developed following the organization's strategy, needs, and policies.

This could result in increased capacity on the part of employees to identify, flag, and mitigate potential SE attacks, establishing safer security behaviors. Of the various approaches analyzed, none of them seems to be completely effective against SE attacks. This is because it becomes difficult to predict human behavior, generating uncertainty and, consequently, making it difficult to find the attack effectively.

Others focus exclusively on the factors and vulnerabilities of humans without referencing defense mechanisms, risks, and techniques/methods of attack. In this sense, it is possible to identify a lack of awareness and training of employees of most organizations regarding issues related to SE. For the same reason, this type of attack can be more successful, calling into question the organization’s Information Security. More comprehensive models are lacking, not only focused on the technical part, on risk or the human component. The SE models should cover all identified areas, gather knowledge of practical experience based on organizational activity and training, and establish standards, using internationally recognized standards and good practices to this end.

In practice, only generic protection measures are found in the analyzed models, but without recourse to international standards and best Information Security practices. In some cases, the models/frameworks found in the literature are outdated compared to the most current SE techniques/persuasion factors.

Regarding the studies analyzed, our systematic review details the most used SE techniques, highlighting the factors that contribute to the success of the attacks. On the other hand, in terms of prevention, it is intended to know in detail which obstacles are referred to in the literature in relation to SE attacks. We differentiate it from traditional systematic review approaches. This framework seeks a comprehensive understanding of the most used SE techniques, not only examining the specific methods of attack but also identifying the factors that contribute to their success.

Furthermore, it aims to examine the most recent prevention frameworks and models in addition to identifying barriers to prevention, offering a more comprehensive picture of the security environment. The last two years' worth of study and literature are the main subjects of the suggested framework. This guarantees that preventive materials and solutions are current, considering the most recent developments and difficulties in the fields of Information Security and SE.

While much research concentrates on attack methods, this framework examines the most recent preventative frameworks and models and places a priority on employee education and ongoing development regarding their understanding of their risks. This shows a dedication to proactive risk reduction and the pursuit of workable ways to stop SE attacks, as opposed to only responding to them. In addition, this endeavor involves assessing the efficacy of current preventative measures, identifying gaps in the literature, and making recommendations for next safety practices and research.

In conclusion, the research that has been evaluated offers significant new perspectives on SE within organizations. To raise awareness and strengthen defenses against SE attacks, they address threats, mitigation techniques, instructional resources, and models. The comprehension and creation of efficient Information Security procedures to prevent employees from psychological manipulation and the leakage of private data on organizations are aided by these findings. We have found gaps in the literature based on these findings. It is crucial to remember that these gaps offer a chance for more study and technical developments in this field.

Our proposed framework can illustrate the relationship between these two characteristics by providing specifics on SE approaches and preventative techniques. This can point out places where a thorough grasp of attack methods can improve defense tactics, and vice versa. To fill in these gaps, we propose a new framework that draws on international standards' best practices and addresses the gaps identified in the literature.

7- Proposed Framework

Based on the previous analysis of the literature, Figure 11 illustrates the proposed framework that aims to be integrative, comprehensive, and adaptable in the various disciplines of the SE, according to the needs of each organization. Considering standards and best practices, types, and techniques of attack, as well as the various targets, this model can focus on and help define the training needs of the employees to be permanently aware of potential SE threats while developing their activities.

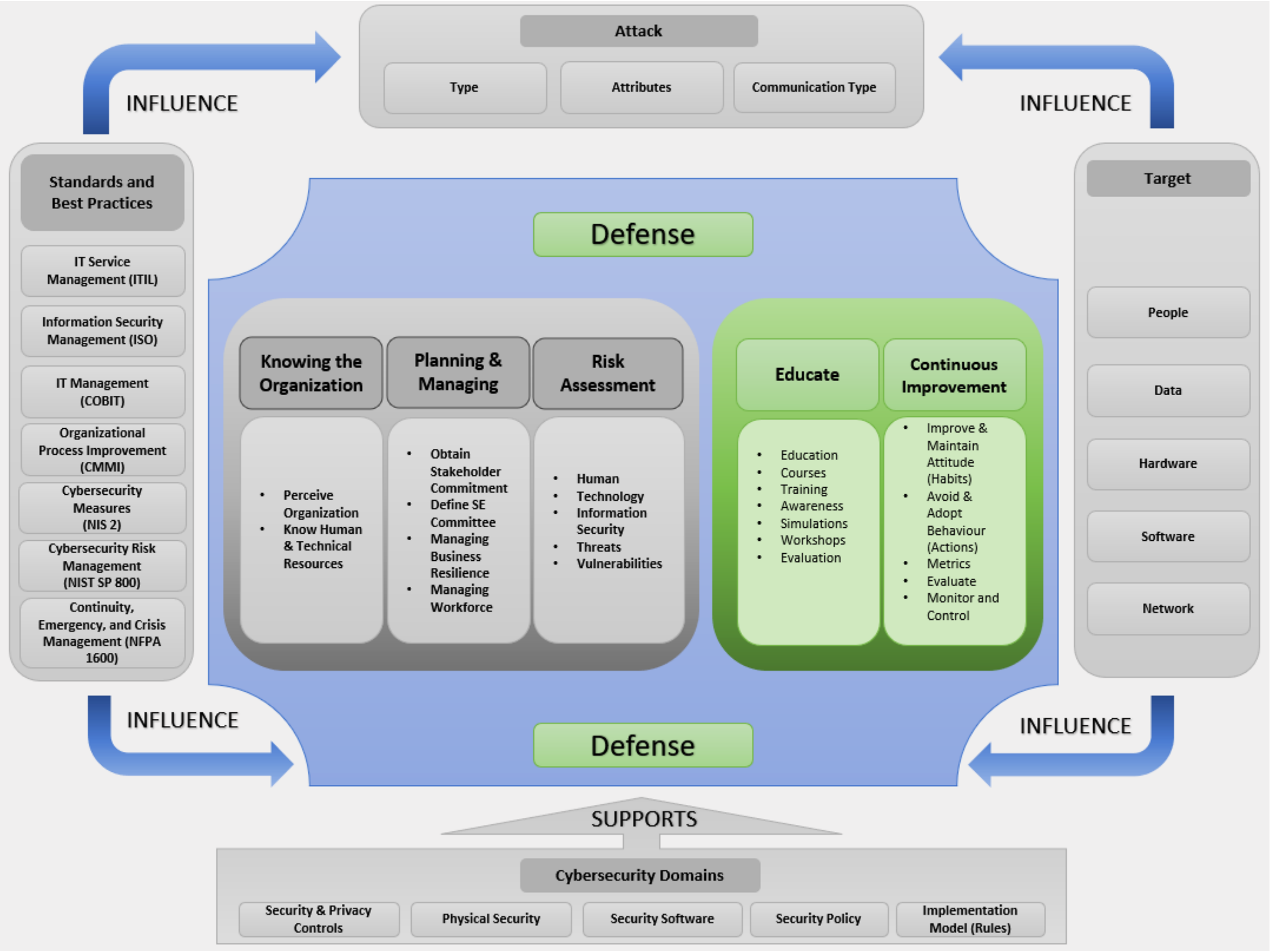

Figure 11. Proposed framework for the prevention of SE attacks

As we can see above, the framework involves several components, but its focus lies in two components identified with green color: *Educate and Continuous Improvement*.

The ***Attack*** component is related to the various types of attacks, their attributes, and the types of communication referred to in the literature.

The ***Target*** component relates to the various types of targets that can be attacked using the exploitation of their vulnerabilities.

The ***Standards and Best Practices*** *and* ***Cybersecurity Domains*** components aim to support the defense component, the focus of this work, referring to internationally recognized best practices, as well as the ***Security & Privacy Controls, Physical Security, Security Software, Security Policy, and Implementation Model (rules).***

Generically, this proposal intends to aggregate the areas of education and continuous improvement, where the various authors detected more gaps in the literature. The two components with the most focus will be briefly described below.

7-1- Educate

This component involves employee education in the SE context, which should involve all organizational levels, including top, intermediate, and operational, addressing areas like courses, training, awareness, simulations, workshops, and evaluation. Through the previous chapter, it was possible to verify that the education and training of employees are crucial to avoiding potential SE attacks and, consequently, organizational risks in the context of Information Security.

7-2- Continuous Improvement

This component is related to the need for employees to be continuously aware of potential threats. In this sense, it is pertinent to ensure the continuous improvement of the current state of the prevention level and its monitoring. For this, organizations can perform, for example, simulations of various scenarios, attacks, or serious games in the work context, observing and subsequently evaluating and monitoring the score results at the individual and collective levels.

7-3- Application of the framework in a hypothetical scenario

This section aims to briefly describe an example of a hypothetical scenario of practical application of this model, where the knowledge of employees to deal with potential attack situations is tested. Let us imagine a certain organization that already has current technological mechanisms for detecting SE attacks but that, nevertheless, has noticed an increase in attacks based on the exploitation of human vulnerabilities. In the last four months, the organization has suffered from 14 attempted attacks using human vulnerabilities. However, they only used technological prevention methods.

In practice, what is intended to be addressed in this scenario is when the attackers idealize an attack using SE, bypassing advanced organizational technological prevention systems, exploiting human vulnerabilities to obtain the desired information, subsequently preparing the attack, and reinforcing themselves, even without recourse to technological means. Currently, the organization does not have any prevention plan for its employees, namely in the context of SE and human vulnerabilities. There were, for example, collaborators who indicated their access credentials to malicious people who contacted them and revealed confidential information by phone to unknown persons. They thought they were colleagues from other departments in other locations, but nevertheless, they were attackers. This type of attack results in breaches of Information Security and can cause damage to the integrity of the information.

In this sense, there was a need to train its employees in this aspect. Using the proposed framework, the organization has verified in the *Educate* component that it could, for example, conduct a questionnaire to this set of collaborators.

In this way, it would be possible to assess their knowledge regarding their behaviors against potential SE threats, namely their own vulnerabilities, in various situations presented and carry out the monitoring of their actions, that is, implementing continuous improvement through monitoring. By analyzing the answers given, the organization can assess the level of maturity at which each employee is in the multiple areas evaluated while determining the level of risk at the same time. After analyzing the results obtained, it was found that only 33% of this set of employees reached a minimum level of knowledge about human vulnerabilities and that many had no idea of the actions they could be committing, unconsciously putting Information Security at risk.

Using the framework, the organization realized this gap and could organize training sessions using a team composed of psychologists (due to the relationship of the SE with psychological factors) and Information Security specialists, considering the vulnerabilities detected. After the various training sessions, which involved knowledge of various attack techniques used by attackers and human persuasion factors, employees became aware of this theme. After 6 months, recurring to the Continuous Improvement component, the organization has monitored results. They can notice a 73% reduction in SE attacks based on the human element and, consequently, the associated risk. In practice, after training and applying prevention and security best practices, it becomes more difficult for an attacker to utilize human persuasion factors to execute the attack. The level of maturity in terms of Information Security has increased, and security breaches through the human element have been reduced.

8- Conclusions

This SLR helps understand SE attacks' potential impacts on organizations, as human elements are weak, and attackers often exploit technological barriers. Existing detection methods and prevention measures have limitations [33], and human-based techniques are subjective and technology-based techniques can be limited. Attackers exploit victims' vulnerabilities for confidential information. Models and frameworks for risk assessment, measurement, and SE attack attributes were identified. The analysis also highlighted the main entities and alignment of SE concepts. Literature provides models and frameworks for preventing SE attacks in organizations, guiding good practices, and mitigating risks. The SLR analysis reveals current research in SE techniques, success factors, models, and prevention measures, highlighting the vulnerability of human vulnerabilities to attackers without technical knowledge.

Organizations need to emphasize the need for new detection techniques and prevention measures based on training actions to minimize employees' inertia and address gaps in current Information Security policies, such as the lack of effective social network use and associated threats. Lack of organizational knowledge about SE and attacker techniques increases the likelihood of successful attacks, making it difficult to accurately assess and obtain security requirements for risk analyses [12].

The literature emphasizes the importance of collaboration training, ethical training programs, employee privacy, and Information Security, as each employee is responsible for their organization's Information Security. Security workshops within organizations are crucial for employees to protect themselves against attackers. Regular strengthening is necessary to prevent relapses and prepare participants for future security threats. These workshops can help mitigate SE attacks based on simulating attacks against employees. However, consideration should be given to the ethical aspect of these attacks, which may be an obstacle to training by some users, who may understand them as an invasion of their privacy [28].

This research highlights the challenges organizations face in addressing security threats (SE) directed at the human element. It highlights the use of SE techniques, success factors, and obstacles while also providing protection measures and an understanding of the threat concept. There is a lack of knowledge and application of best practices for protecting organizations from cyberattacks. Future research could benefit from SE attack prevention frameworks and replicate existing knowledge. With increasingly sophisticated techniques and attacks, there is still room for improvement in new frameworks and understanding their benefits and challenges.

We grouped results to provide an integrated view of previous contributions and contribute to understanding concepts and good practices in Information Security. Our work aims to enhance the development of new frameworks and training techniques to prevent SE attacks. Future research should explore new types of SE attacks, detection models, and employee prevention, training, and education. We suggest future research on new types of SE attacks, updating detection models, preventing, and training employees, and implementing security policies to reduce attack success. This work also emphasizes the need to study human persuasion factors and new ones, as humans are still susceptible to psychological manipulation techniques.

All new techniques must be studied and presented in organizations to increase organizational Information Security. Organizations must study and present new techniques to enhance Information Security (IS). This framework can serve as a basis for developing policies and training programs adapted to each organization's needs. It helps organizations evaluate their maturity level for potential attacks and understand employee training needs. A tool will also be proposed to assess these needs, with future work involving testing and validation.

9- Declarations

9-1- Author Contributions

Conceptualization, A.L. and H.M.; methodology, A.L. and H.M.; formal analysis, A.L. and H.M.; investigation, A.L.; data curation, A.L. and L.R.; writing—original draft preparation, A.L.; writing—review and editing, H.M., L.R., and A.S.; supervision, H.M., L.R., and A.S.; funding acquisition, H.M. All authors have read and agreed to the published version of the manuscript.

9-2- Data Availability Statement

Data sharing is not applicable to this article.

9-3- Funding

This work is financed by National Funds through the Portuguese funding agency, FCT - Fundação para a Ciência e a Tecnologia, within project UIDP/50014/2020. doi:10.54499/UIDP/50014/2020.

9-4- Acknowledgements

The authors wish to thank the Institute for Systems and Computer Engineering, Technology and Science (INESC TEC).

9-5- Institutional Review Board Statement

Not applicable.

9-6- Informed Consent Statement

Not applicable.

9-7- Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

10- References

[1] Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. John Wiley & Sons, Hoboken, United States.

[2] Wilcox, H., & Bhattacharya, M. (2016). A framework to mitigate social engineering through social media within the enterprise. Proceedings of the 2016 IEEE 11th Conference on Industrial Electronics and Applications, ICIEA 2016, 1039–1044. doi:10.1109/ICIEA.2016.7603735.

[3] Kaushalya, S. A. D. T. P., Randeniya, R. M. R. S. B., & Liyanage, A. D. S. (2018). An Overview of Social Engineering in the Context of Information Security. 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences, ICETAS 2018, Bangkok, Thailand. doi:10.1109/ICETAS.2018.8629126.

[4] Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer networks, 51(12), 3448-3470. doi:10.1016/j.comnet.2007.02.001.

[5] Mouton, F., Nottingham, A., Leenen, L., & Venter, H. S. (2017). Underlying finite state machine for the social engineering attack detection model. Information Security for South Africa (ISSA), Johannesburg, South Africa. doi:10.1109/issa.2017.8251781.

[6] Cullen, A., & Armitage, L. (2018). A human vulnerability assessment methodology. 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018, 1–2. doi:10.1109/CyberSA.2018.8551371.

[7] Leonov, P. Y., Vorobyev, A. V., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A. K., & Morozov, N. V. (2021). The Main Social Engineering Techniques Aimed at Hacking Information Systems. 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia. doi:10.1109/usbereit51232.2021.9455031.

[8] Abeywardana, K. Y., Pfluegel, E., & Tunnicliffe, M. J. (2016). A layered defense mechanism for a social engineering aware perimeter. 2016 SAI Computing Conference (SAI), London, United Kingdom. doi:10.1109/sai.2016.7556108.

[9] Gupta, S., Isha, Bhattacharya, A., & Gupta, H. (2021). Analysis of Social Engineering Attack on Cryptographic Algorithm. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021, 1–5. doi:10.1109/ICRITO51393.2021.9596568.

[10] Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-Centric Computing and Information Sciences, 8(1), 1–24. doi:10.1186/s13673-018-0128-7.

[11] Hamoud, A., & Aïmeur, E. (2020). Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model. Frontiers in Computer Science, 2. doi:10.3389/fcomp.2020.00025.

[12] Li, T., Wang, K., & Horkoff, J. (2019). Towards Effective Assessment for Social Engineering Attacks. 2019 IEEE 27th International Requirements Engineering Conference (RE), Jeju, Korea (South). doi:10.1109/re.2019.00051.

[13] Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., & Wei, Z. (2021). Understanding and deciphering of social engineering attack scenarios. Security and Privacy, 4(4), 1–17. doi:10.1002/spy2.161.

[14] Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, NSW, Australia. doi:10.1109/tale.2018.8615162.

[15] Esparza, J., Caporusso, N., Walters, A. (2020). Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools. Advances in Human Factors in Cybersecurity. AHFE 2020. Advances in Intelligent Systems and Computing, 1219. Springer, Cham, Switzerland. doi:10.1007/978-3-030-52581-1_12.

[16] Kitchenham, B. (2004). Procedures for performing systematic reviews. NICTA technical Report 0400011T.1, Keele University, Keele, United Kingdom.

[17] Bryant, B. R., & Seok, S. (2017). Introduction to the special series: Technology and disabilities in education. Assistive Technology, 29(3), 121–122. doi:10.1080/10400435.2016.1230154.

[18] de Freitas, M. P., Piai, V. A., Farias, R. H., Fernandes, A. M. R., de Moraes Rossetto, A. G., & Leithardt, V. R. Q. (2022). Artificial Intelligence of Things Applied to Assistive Technology: A Systematic Literature Review. Sensors, 22(21), 8531. doi:10.3390/s22218531.

[19] Kitchenham, B. A., Charters, S. M. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report, EBSE-2007-01, Keele University, Keele, United Kingdom.

[20] Banijamali, A., Pakanen, O. P., Kuvaja, P., & Oivo, M. (2020). Software architectures of the convergence of cloud computing and the Internet of Things: A systematic literature review. Information and Software Technology, 122, 106271. doi:10.1016/j.infsof.2020.106271.

[21] Hijji, M., & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions. IEEE Access, 9, 7152–7169. doi:10.1109/ACCESS.2020.3048839.

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

[23] Borkovich, D. J., & Skovira, R. J. (2019). Cybersecurity Inertia and Social Engineering: Who's Worse, Employees or Hackers? Issues in Information Systems, 20(3), 139–150. doi:10.48009/3_iis_2019_139-150.

[24] Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. IEEE Access, 8, 85094–85115. doi:10.1109/ACCESS.2020.2992807.

[25] Alharthi, D.N., Regan, A.C. (2020). Social Engineering Defense Mechanisms: A Taxonomy and a Survey of Employees' Awareness Level. Intelligent Computing. SAI 2020, Advances in Intelligent Systems and Computing, 1228, Springer, Cham, Switzerland. doi:10.1007/978-3-030-52249-0_35.

[26] Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. Procedia Computer Science, 198, 656-661. doi:10.1016/j.procs.2021.12.302.

[27] Rege, A., Williams, K., & Mendlein, A. (2019). A Social Engineering Course Project for Undergraduate Students Across Multiple Disciplines. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, United Kingdom. doi:10.1109/cybersecpods.2019.8885085.

[28] Rege, A., Nguyen, T., & Bleiman, R. (2020). A social engineering awareness and training workshop for STEM students and practitioners. IEEE Integrated STEM Education Conference, Princeton, United States. doi:10.1109/isec49744.2020.9280596.

[29] Alharthi, D.N., Hammad, M.M., Regan, A.C. (2020). A Taxonomy of Social Engineering Defense Mechanisms. Advances in Information and Communication. FICC 2020. Advances in Intelligent Systems and Computing, 1130, Springer, Cham, Switzerland. doi:10.1007/978-3-030-39442-4_3.

[30] Hadnagy, C., & Fincher, M. (2015). Phishing dark waters: The offensive and defensive sides of malicious Emails. John Wiley & Sons, Hoboken, United States. doi:10.1002/9781119183624.

[31] PÎRNĂU, M. (2017). Considerations on preventing social engineering over the internet. Memoirs of the Scientific Sections of the Romanian Academy, Tome XL.

[32] Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks. Advances in Information Security, Privacy, and Ethics, 19–31, IGI Global, Pennsylvania, United States. doi:10.4018/978-1-7998-6504-9.ch002.

[33] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. doi:10.3390/FI11040089.

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

[35] Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. Cybersecurity, 4(1), 1–21. doi:10.1186/s42400-021-00094-6.

[36] Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. International Journal of Computer Network and Information Security, 9(1), 1–11. doi:10.5815/ijcnis.2017.01.01.

[37] Mattera, M., & Chowdhury, M. M. (2021). Social Engineering: The Looming Threat. 2021 IEEE International Conference on Electro Information Technology (EIT), Michigan, United States. doi:10.1109/eit51626.2021.9491884.

[38] Kamruzzaman, A., Thakur, K., Ismat, S., Ali, M. L., Huang, K., & Thakur, H. N. (2023). Social Engineering Incidents and Preventions. 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, United States. doi:10.1109/ccwc57344.2023.10099202.

[39] Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India. doi:10.1109/ccaa.2016.7813778.

[40] Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys, 48(3), 1-39. doi:10.1145/2835375.

[41] Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A risk analysis framework for social engineering attack based on user profiling. Journal of Organizational and End User Computing, 32(3), 37–49. doi:10.4018/JOEUC.2020070104.

[42] Arya, B., Chandrasekaran, K. (2016). A client-side anti-pharming (CSAP) approach. Proceedings of the 2016 IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), 23–24 November 2015, Nagercoil, India.

[43] Zheng, K., Wu, T., Wang, X., Wu, B., & Wu, C. (2019). A Session and Dialogue-Based Social Engineering Framework. IEEE Access, 7, 67781–67794. doi:10.1109/ACCESS.2019.2919150.

[44] Obuhuma, J., & Zivuku, S. (2020, May). Social engineering based cyber-attacks in Kenya. 2020 IST-Africa Conference (IST-Africa), 18-22 May, 2020, Kampala, Uganda.

[45] Mattera, M., & Chowdhury, M. M. (2021). Social Engineering: The Looming Threat. 2021 IEEE International Conference on Electro Information Technology (EIT), Michigan, United States. doi:10.1109/eit51626.2021.9491884.

[46] Alyahya, A., & Weir, G. R. S. (2021). Understanding Responses to Phishing in Saudi Arabia via the Theory of Planned Behaviour. 2021 National Computing Colleges Conference (NCCC), Taif, Saudi Arabia. doi:10.1109/nccc49330.2021.9428823.

[47] Gomes, V. A. N. (2019). Social Engineering and the Dangers of Phishing. Master Thesis, ISCTE-Instituto Universitario de Lisboa, Lisbon, Portugal. (In Portuguese).

[48] Ozkaya, E. (2018). Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert. Packt Publishing Ltd, Birmingham, United Kingdom.

[49] Ferreira, A. (2018). Why Ransomware Needs A Human Touch. 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, Canada. doi:10.1109/ccst.2018.8585650.

[50] Tu, H., Doupe, A., Zhao, Z., & Ahn, G.-J. (2016). SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam. 2016 IEEE Symposium on Security and Privacy (SP), San Jose, United States. doi:10.1109/sp.2016.27.

[51] Duarte, N., Coelho, N., Guarda, T. (2021). Social Engineering: The Art of Attacks. Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2021. Communications in Computer and Information Science, Volume 1485. Springer, Cham, Switzerland. doi:10.1007/978-3-030-90241-4_36.

[52] Cardoso, W. R., Silva, J. M., & Ribeiro, A. R. L. (2023). An Expert System as an Awareness Tool to Prevent Social Engineering Attacks in Public Organizations. International Journal on Cybernetics & Informatics, 12(5), 61–70. doi:10.5121/ijci.2023.120506.

[53] Alzahrani, A. (2020). Coronavirus social engineering attacks: Issues and recommendations. International Journal of Advanced Computer Science and Applications, 11(5), 154–161. doi:10.14569/IJACSA.2020.0110523.

[54] Li, T., Wang, X., & Ni, Y. (2022). Aligning social concerns with information system security: A fundamental ontology for social engineering. Information Systems, 104. doi:10.1016/j.is.2020.101699.

[55] Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons, Hoboken, United States.

[56] Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. John Wiley & Sons, Hoboken, United States.

[57] Bezuidenhout, M., Mouton, F., & Venter, H. S. (2010). Social engineering attack detection model: SEADM. 2010 Information Security for South Africa, Johannesburg, South Africa. doi:10.1109/issa.2010.5588500.

[58] Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. doi:10.1111/j.1083-6101.2007.00393.x.

[59] Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking sites. IEEE Security and Privacy, 5(3), 40–49. doi:10.1109/MSP.2007.75.

[60] Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N. (2015). Mitigating social engineering for improved cybersecurity. 2015 International Conference on Cyberspace (CYBER), Abuja, Nigeria. doi:10.1109/cyber-abuja.2015.7360515.

[61] Foozy, C. F. M., Ahmad, R., Abdollah, M. F., Yusof, R., & Mas'ud, M. Z. (2011, November). Generic taxonomy of social engineering attack and defence mechanism for handheld computer study. Malaysian Technical Universities International Conference on Engineering & Technology, 13-15 November, 2011, Batu Pahat, Johor.

[62] Cullen, A., & Armitage, L. (2016). The social engineering attack spiral (SEAS). 2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), London, United Kingdom. doi:10.1109/cybersecpods.2016.7502347.

[63] Aldawood, H., & Skinner, G. (2019). An academic review of current industrial and commercial cyber security social engineering solutions. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, 110-115. doi:10.1145/3309074.3309083.

[64] Saleem, J., & Hammoudeh, M. (2017). Defense methods against social engineering attacks. Computer and Network Security Essentials, Springer International Publishing, 603–618. doi:10.1007/978-3-319-58424-9_35.

[65] Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 128, 113160. doi:10.1016/j.dss.2019.113160.

[66] Aldawood, H., & Skinner, G. (2019). Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. Cybersecurity and Cyber forensics Conference (CCC), Melbourne, Australia. doi:10.1109/ccc.2019.00004

[67] Bakhshi, T. (2017). Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. 2017 13th International Conference on Emerging Technologies (ICET), Islamabad, Pakistan. doi:10.1109/icet.2017.8281653.

[68] Elmrabit, N. (2018). A multiple-perspective approach for insider-threat risk prediction in cyber-security. Ph.D. Thesis, Loughborough University, Loughborough, United Kingdom.

[69] Grant, R. L. (2017). Exploring effects of organizational culture upon implementation of information security awareness and training programs within the defense industry located in the Tennessee valley region. Ph.D. Thesis, Florida Institute of Technology, Melbourne, United States.

[70] Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. Computers in Human Behavior Reports, 4. doi:10.1016/j.chbr.2021.100126.

[71] Duman, Ş. A., Hayran, R., & Sogukpinar, İ. (2023). Impact Analysis and Performance Model of Social Engineering Techniques. 2023 11th International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, United States. doi:10.1109/isdfs58141.2023.10131771.

[72] Öztürk, A., Koza, E., & Willer, M. (2023). Social Engineering Penetration Testing within the OODCA Cycle – Approaches to Detect and Remediate Human Vulnerabilities and Risks in Information Security. AHFE International, Volume 91, United States. doi:10.54941/ahfe1003721.

[73] Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50. doi:10.1016/j.cosrev.2023.100592.