International Journal of Science and Engineering Invention (IJSEI)
Volume 08, Issue 02, February 2022,
https://doi.org/10.23958/ijsei/vol08-i02/226

Original article

Social Engineering Attack Concepts, Frameworks, and Awareness: A Systematic Literature Review

Ruwa F. Abu Hweidi *[1], Derar Eleyan [2]

[1]M.S. Student, Palestine Technical University-Kadoorie (PTUK), Faculty of Graduate Studies, Specializ-ing Cybercrimes and digital evidence analysis, Tulkarm, Palestine; *r.f.abuhweidi@students.ptuk.edu.ps*

[2]Associate Professor, Palestine Technical University- Kadoorie (PTUK), Department of Applied Com-puting, Tulkarm, Palestine; *d.eleyan@ptuk.edu.ps*

*Corresponding Author: Ruwa F. Abu Hweidi; *r.f.abuhweidi@students.ptuk.edu.ps*

Received 01 January 2022; Accepted 27 January 2022; Published 02 February 2022

Abstract

Social engineering attacks occupy high percentage of total cybercrimes. It is also classified as the major cause of financial losses in cyberspace. This shows the need to clarify social engineering definition and clarify the proposed frameworks solutions by different re-searchers. This paper explores the previous researches that try to extract different concepts and perspectives of frameworks, knowing this and the development of the framework help us face the threat of social engineering. Most of the studies agree on the effect of a comprehensive framework and how it affects positively. The results express the need for more empirical stud-ies, government permissions, financial support to improve the conceptual frameworks to apply them to a wide range of societies, and more focus on awareness responsibility for government, users, and organizations. This paper agrees the previous results and emphasizes the need for empirical comprehensive conceptual framework and government support.

Keywords: ***Attack, awareness, cybercrime, cybersecurity, cyberspace, framework, lifecycle, model, phase, and social engineering.***

1. Introduction

Societies look forward to living in a high level of privacy and security in both actual life and cyberspace. Cyberspace occupies a wide part of our lives such as social media, e-commerce, e-learning, and financial transactions, therefore as there are thieves who exploit human vulnerabilities in real life, there are hackers in cyberspace called social engineers, who applies many attacks via different techniques and tools which called social engineering (SE) attacks.

SE attacks are the most frequent cyberattacks type of cybercrimes comparing to other types of attacks according to ISACA report in 2021 which shows SE as the most frequent cyberattack [1], moreover, SE oc-cupied 98% of cybercrimes according to Purplesec cyber security statistics report in 2021 [2]. According to FBI internet crime report in 2020, the victims lost more than 4.2 Billion dollars [3]. Thus, SE attacks caused big financial problems to countries and citizens.

Specialists and consultant managers in organizations and governments are trying to develop tools to face these types of attacks away from traditional methods such as intrusion detection and prevention techniques and tools to limit the effect of this type of crime. So, it's important to construct a clear understandable base to decrease SE attacks risks conducted through various attack types such as phishing, vishing, spear phishing, and smishing, etc [4-7]. That is achieved by describing SE attacks comprehensively in an obvious conceptual framework.

This study reviews the concept of SE in cybersecurity and part of frameworks that exist in the eligibility criteria of research methodology and discusses the awareness needs on both human and government levels.

The previously reviewed studies try to extract different concepts and perspectives which are called lifecycles, phases, frameworks, models, or a mix of them. Understanding these concepts and perspectives, and the development of frameworks help us face the threat of social engineering. Most of the studies agree on the effect of a comprehensive framework and how it affects positively. In awareness criteria, the results express the need for more empirical studies, government permissions, financial support to improve conceptual frameworks to apply them to a wide variety of societies and focus more on awareness responsibility of government, users, and organizations. The contributions of this paper are:

1) Give a comprehensive view of previous studies for the concepts and frameworks of SE, therefore, how this affects the awareness trend.
2) Discuss the results and explore findings, limitations, risks of bias, and future work in each study.
3) Show in detail the phases of the framework of SE attacks in studies in eligibility criteria, and how it developed, then initialize the connection between them inclusively as future work.
4) Show the lack of empirical studies in this topic, to build an inclusive model with a comprehensive perspective.
5) Indicates how such studies need government funds and the right to access the information.
6) Propose some future work depending on the results that may meet the objectives of the researchers in the future.

And suggest a conceptual framework to do a wide comparative study to build an integrated framework and include the mitigation countermeasure within.

This study is classified as A systematic literature review (SLR) which is committed in Prisma 2020 statement [8] and follows its checklist step by step and framework flow diagram as shown in Fig. 1, then reports as a systematic review.

The rest of the paper is organized as follows: Section 2 discusses the methods that are used in detail ac-cording to Prisma methodology [8]. Section 3 explains the results inclusively. Section 4 is the discussion of results. Finally, section 5 the conclusion and future work.

2. Methods

This is an SLR paper, which uses Preferred Reporting Items for Systematic Reviews and Meta-Analysis (Prisma) 2020 [8]. SLR type described as qualitative SLR, which have an objective of explaining the concept of SE and how SE attack framework (lifecycles, phases, or models) developed through last 7 years, to give a literature review to where researchers reach this dynamic topic by gathering reviews and analyzing them, as well as, the contribution to increase awareness.

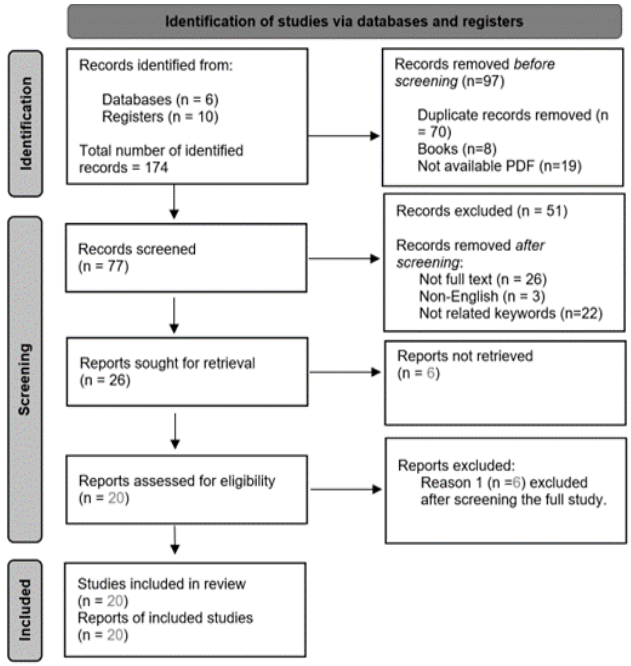

Fig. 1. Prisma framework flow diagram.

2.1 Identification or Eligibility Criteria

Firstly, the study searches google scholar to look for SE attacks in general, to know the most related key-word used in academic research databases in SE. Then, it searches in various engines and databases e.g., available open access journals, and conferences, looking for specific keywords and synonyms to take an overview. The search went in-depth in databases using different filters to filter results, such as related stud-ies in English language in the period between 2014 and 2022, and computer science field. The chart in Fig. 2 shows the distribution of Publication through the years in this SLR.

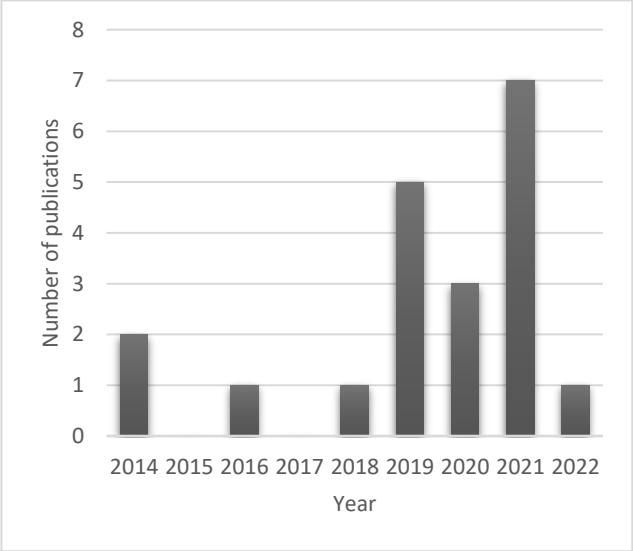

Fig. 2. Distribution of Publication through the years.

2.2 Information Source and Search Strategy

Table 2 specifies eligibility and determines the inclusion and exclusion criteria in SLR. shows several findings in each source, with the following details:

1) The main engines and databases used are Elsevier, Foundation of Computer Science, IEEE, IGI Global, MDPI AG, Scientific Research Publishing, Springer, Publishing Group Ltd/Prisma, and Wiley.
2) Three websites: FBI, ISACA, and Purplesec.
3) The keywords and synonyms used are: “Social engineering”, “attack*”, “cybercrime”, “scenarios”, “framework”, “technique”, “model”, “lifecycle”, “phases”, “concept”, “taxonomy”, “mechanism”, “definition”, “mitigation”, “prevention”, “scam”, “type”, “*phishing”.
4) The filters used in search are:
    a. Publication types: Journal and conference.
    b. Year: 2014-2022.
    c. Publication topic: Computer science and cybercrime.
    d. Article Versions: Full-text PDF.
    e. Language: English
    f. Boolean operator: OR, AND.

Table 2 specifies eligibility and determines the inclusion and exclusion criteria in SLR.

Table 1: Databases & keywords

Publisher	Articles	Keywords
Elsevier	3	“Social engineering”, “attack*”, “cybercrime”, “scenarios”, “framework”, “technique”, “model”, “lifecycle”, “phases”, “concept”, “taxonomy”, “mechanism”, “definition”, “mitigation”, “prevention”, “scam”, “type”, “*phishing”.
Foundation of Computer Science	1	
IEEE	7	
IGI Global	1	
MDPI AG	2	
Scientific Research Publishing	1	
Springer	1	
Wiley	1	
Sites	3	

Table 2: Inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Period	2014-2022	Less than 2014
Access	Full/ open access	Close access/ with permission
Language	English	Other languages
Keywords	One related keyword at least	No keyword matches
Type of study	journals, conferences, and 3 sites	Others
publication topic	computer science & cybercrime	Others sections
Downloadable	PDF files	Others
Information	Full	Others

2.3 Selection and Data Collection Process

In the selection and data collection process, SLR screened and conducted previous stages which measured on eligibility criteria, Fig 2 showed the Prisma framework flow diagram. The identified records were n=174 from different databases such as Web of Science, IEEE, ScienceDirect and google scholar. The total Records removed before screening was n=97 (Duplicate records removed (n=70), Books (n=8), Not availa-ble PDF (n=19)), 51 records were excluded (Not full text (n=26), non-English (n=3), Not related to SE (n=22)) from 77 records screened, therefore, a total of reports sought for retrieval was n=26, reports not re-trieved n=6, after those 20 eligible papers were included in present SLR. There were three paper types dis-tributed as 80% Qualitative, 15% Quantitative, and 5% mix of both, as shown in Fig. 3.

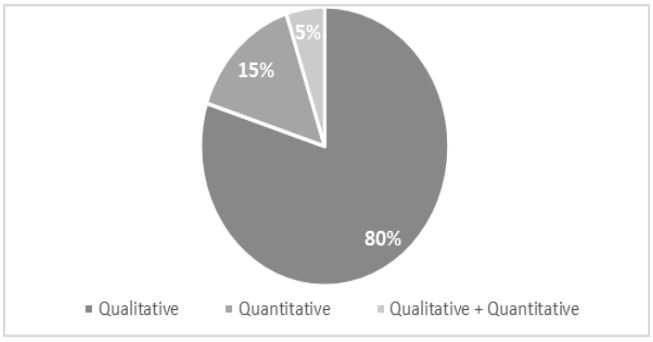

Fig. 3. Studies type distribution.

2.4 Limitations and Risk of Bias in the search strategy

This paper reviewed studies from 2014 through 2022 most of them during 2021, but faced three types of limitations that increased the risk:

1) Availability of information: Many of the studies are not available for free, or not accessible in data-bases, so the search used different databases to decrease the effect of this risk.
2) Repetition of author's name: some authors who are interested in SE have different related papers in the search scope, thus, this paper takes the newest study on the same topic as it possible, which is subjected to eligibility criteria if possible.
3) Screening: Inclusion and Exclusion files are determined by the article downloadability, and the file type (PDF).

2.5 Data Extraction/ Analytic Strategy

In each step of SLR, all articles were stored in Mendeley reference manager as PDF files, then, exported to Excel sheet to follow Prisma statement to extract and analyze data. Also, each included article should achieve the objective of the study.

3. Results

The number of studies included in the review of the total number of identified records is 20, these are eligi-ble for the SLR by using qualitative synthesis. The SLR finds that the published studies increased in the year 2021. The total number of published studies in 2021 is 35%, 15% in 2020, 25% in 2019, and the total of other years equals 25%. This indicates how challenges increased to focus on and face SE effects, and to find a comprehensive definition and conceptual model.

In previous times Mouton et al. [9] define SE as a science that exploits social interaction by using a computer to achieve the goal of the attacker pursuant humans or organizations. Through years, SE attacks have been a dangerous effect on cyberspace and are classified as the cause of the most financial lose in cy-berspace, and they threat cybersecurity by different techniques such as phishing and spear-phishing [1-3], consequently, SE takes part of researchers' interest and challenges them to find a full concept for SE in cyberspace as relevant to cybercrime.

Wang et al. [10] tried to find an inclusive definition by evaluating, analyzing, and discussing surveys that debate the concept of SE, according to that, the advantages and disadvantages of each analysis results con-tribute to the followed methodology to define SE from different views and theories, the proposed definition said: ''Social engineering in cybersecurity (SEiCS) is a type of attack where in the attacker(s) exploit hu-man vulnerabilities using social interaction to breach cyber security''.

In the objective of this SLR, there are selected studies focused on extracting and analyzing data theoreti-cally or practically and tried to find a comprehensive framework that expresses the SE concept from differ-ent perspectives. They used different words to express this objective like phases, lifecycle, model, and framework [11-17], this emphasizes the importance of increasing researches in this field as future work, and how these frameworks affect in raising awareness, by giving inclusive view to SE attacks on the other hand, this concludes the need to adopt training programs, educational system, and laws to increase awareness among citizens [4-7,18-22]. Summaries for parts of the phases and conceptual frameworks and their methodology types in included studies are in Table 3. And all of findings, limitations, risks of bias, and future work for each SE attack framework in the included studies are summarized in Table 4.

Wang et al. [11] suggest a model that consists of three main entities called perspectives used to explain, follow up the SE attackers and how they deceive victims, the first one is interested in more than forty hu-man vulnerabilities and psychological aspects that are part of human nature, which summarized in six concepts i.e., 1) cognition and knowledge, 2) behavior and habit, 3) emotions and feelings, 4) human nature, 5) personality traits, and 6) individual characters, the second element is the techniques that attackers used to create linkage with the victim, which contains six mechanisms resulted from summarizing more than thirty effect mechanisms, i.e., 1) persuasion, 2) social influence, 3) cognition, attitude, and behavior, 4) trust and deception, 5) language, thought, and decision, 6) emotion and decision-making, the final part focuses on thirteen approaches to apply sixteen attack scenarios, i.e., pretexting, vishing, shoulder surfing, manipulating conversation, piggybacking, trailing, impersonating, baiting, phishing, smishing, trojan attack or honey trap, water-holing, and reverse social engineering.

Table 3. Summary for part of the phases and conceptual frameworks and their types in included studies

Study	Type of study	Summary
[11] Wang et al.	Model as perspectives	This article offers a conceptual model with 3 perspectives (attack methods, 16 SE attack scenarios are presented, over 30 mechanisms of effect and over 40 human vulnerabilities are summarized) where social engineering attacks take effect are analyzed and discussed understand how social engineering attacks work and take effect.
[12] Karadsheh *et al.*	Model as phases	This study result is a model for SE attacks depending on 8 phases (identification of the potential target, target recognition, decision approach, and execution, information aggregations, analysis and interpretation, armament, and influencing), the first 5 phases partly have an effect in security countermeasure, and the others completely have an effect.
[13] Mouton *et al.*	Framework as phases	Mouton's framework contains 6 phases full of Attack formulation, information gathering, preparation, developing a relationship, exploiting the relationship, and debrief. The author depends on his ontological model and Kevin Mitnick's social engineering attack cycle [23] to rebuild a new framework with more details. Mitnick's cycle contains 4 phases, Research, Development of rapport and trust, Exploiting the trust, Utilized information.
[14] Mouton *et al.*	Apply framework in templates	This paper discovered social engineering as a domain and social engineering attacks as a process in it, by using real scenarios and applying it in 6 phases which presented in the last studies for author depend on 6 features: goal, medium, social engineer, target, compliance principles and techniques [9,13].
[15] Yasin *et al.*	Apply framework inactivity	Proposed an analysis model of social engineers that covers how social engineers do information collection, organize the attack cycle, and key principles being applied, the phases listed are: gathering information, medium-contacting the victim, executing the tactic, persuasion-taking advantage of psychology weakness, and then achieving the goal, furthermore suggest activities that decrease SE effect.
[16] Zheng *et al.*	Framework as sessions and dialogs	Proposed a framework consisting of three phases: attack preparation, attack implementation, attack gain. Those phases are repeated in two graphs: SE session (SES), and SE dialog (SED) which is repeated multiple times inside the attack implementation phase of the SES graph.
[17] Washo	Framework as a diagram	Proposed framework as a diagram for use in future studies, hang on philosophical or practical ethics perspective, which consists on core SE susceptibility in organization with three-level encircled: physiology, information technology, and business

Table 4. Finds, limitations, risk of bias, and future works for each SE attack framework in included studies

Study	finds	Limitations	Risk of bias	Future works
[11] Wang et al.	Presents a conceptual model with 3 perspectives to know how SE attacks works and their effects.	Discusses effects (e.g., human vulnerabilities) theoretically, non-empirical	Theoretical perspectives	study the model empirically, the domain ontology of social engineering, and its knowledge graph application.
[12] Karadsheh *et al.*	Presents a new model of SE attack with 8 phases. A quantitative study by using survey data.	The sample size is small which is restricted to 3 companies so the results depend on population culture.	Bias based on Demographic information distributed non-equal. (e.g., gender, age)	improve the model and security countermeasures.
[13] Mouton *et al.*	Proposed framework for SE attack with 6 phases.	The proposed framework depends on one study, and test it in a small sample size.	Theoretical no distinguish between attacks (technical/ non-technical)	Wide empirical examination studies.
[14] Mouton *et al.*	Templates for real scenarios are applied to the framework in [13].	A small sample of template scenarios	Based on theoretical study	Wide empirical examination studies.
[15] Yasin *et al.*	Presents analysis model with 5 phases.	The analyzed model presents a small part of society and the SE scenarios vary depending on Demographic information	Bias based on Demographic information distributed	Gathering and examining more diverse real-life attack scenarios.
[16] Zheng *et al.*	Presents framework of SES and multiple SED inside it.	Used theoretical prove to formalize the framework.	Does not specify what action to take if a dialog failed.	Apply framework empirically to a wide-ranging real network.
[17] Washo	Proposed framework depends on a practical ethics perspective.	Does not give a clear perspective of SE attacks flow.	Theoretical	Apply framework empirically to a wide-ranging real network.

Also, the study gives one case study to approve that model and it is restricted in theoretical aspects, then the study explains some dropped entities like the attack medium and the relation between entities, at last, suggests studying the domain ontology of SE and its knowledge graph application [11].

Karadsheh et al. [12], try to solve the shortage in sub-details in technical attack strategies in each pro-posed phase for SE attacks in previous studies to increase the security by knowing the attacker techniques, then the study puts hypotheses and tests them empirically using a questionnaire among the employees of three companies, then depending on hypotheses the study constructs a

model which contains three varia-bles: 1) independent variables called SE attack phases, which includes eight sub-phases are identification of the potential target, information aggregations, analysis and interpretation, target recognition, decision approach, armament, influence, and execution, 2) mediating variables are called SEI, 3) dependent varia-bles called improved security countermeasures.

The authors [13] use Kevin Mitnick's SE attack cycle [23] and highlight the gaps in lack of details in the phases and the relation between them, then use a previous ontological model for SE attack for the author [9]. All of that to build a framework as appears in these six phases, 1) Attack Formulation which contains goal and target identification, 2) Information Gathering which has three elements that have interrelation-ship between each other, are (identify the potential source, and gather information from source then assess it), 3) Preparation phase that has combination and analysis of gathered data, then the development of an attack vector which may go to previous or next phase, 4) Develop a Relationship that includes the estab-lishment of communication and rapport building, then 5) Exploit the Relationship by priming the target then elicitation it, and finally, 6) Debrief, in this phase there are maintenance and transition which ending in goal satisfaction or back to the preparation stage, so the study proposed that rise up conscious and possi-bility to give a good explanation for SE attack [13].

This study by Mouton et al. [14] explores SE attack scenarios by tracing and analyzing scenarios of at-tacks through a model that has six phases in a template for each type of attack [13]. In detail, the study tries to evaluate and approve the SE attack model by accessing attacks in a template to facilitate the detection of attack then deal with it, increasing conscious of societies, and use it in educational goals, but without dis-tinguishing the taxonomy of attack as technical or non-technical [14].

Yasin et al. [15] proposed an analysis model of social engineers depending on real scenarios, which co-vers how social engineers do information collection, organize the attack cycle, and key principles being applied, the phases listed are: gathering information, medium-contacting the victim, executing the tactic (scenario), a persuasion-taking advantage of psychology weakness, and then achieving the goal, further-more suggest activities that decrease SE effect, besides that, the paper views each attack method from the attacker and victim perspectives and analyzes the principles of attack techniques and the vulnerabilities of the victim.

Zheng et al. [16] Proposed a framework consisting of three phases: attack preparation, attack implementation, and attack gain, those phases are repeated in two graphs: SE session (SES), and SE dialog (SED), and SED is repeated multiple times inside the attack implementation phase of the SES graph depending on the attack technique; in detail, the first phase in SES is preparation which consists of the following steps: 1) attack goal which depends on preparation step in SED and works as a leader in each step to achieve the aim of SE attack, 2) attack preparation level that includes all of the preparation steps of SED, 3) toolkit, 4) session scenario, in the last two steps; the SE collecting a comprehensive study, and the data required to proceed the attack, as well as, the second step is the core of SES which allow repeating SED several times within, with the same phases of SES, Finally the attack gain phase that consists of results of attack and if the attacker reaches his objectives or not, so the arrangement of SED inside SES is important in the SE at-tack to bring down the victim and reach the goal.

The study of Washo [17] focused on the ethical concept in the proposed framework as a diagram for use in future studies, introducing philosophical or practical ethics perspective, which consists of core SE susceptibility in organization with three levels encircled: physiology, information technology, and business.

The limitations and risk of bias in included studies that proposed its frameworks depending on theoretical analysis, with a limited number of case studies approved [11,14-17]. Empirical analysis with a small sample size of humans depends on limited factors such as age, gender, etc [12]. Or scenarios in real-time which have a bias based on Demographic information distributed [12,15]. The detailed summaries are in Table 4.

The last objective of this LSR is interested in awareness, to explain the effect of the main need to face SE attacks, after the review shows concepts of SE in cybersecurity and part of frameworks, here are parts of the studies interested in awareness [4,6,7,18-22] the details are:

Aldawood in [18] explores the reasons that affect the staff of the organization to face SE attacks, such as training and awareness, this study found an increase in weaknesses if the organization depends on the inte-gration of information systems, therefore, the risk rises.

Noteworthy, SE attacks developed in parallel with technical movement and countermeasures. Addition-ally, the paper proposes different ways to reduce employee training costs, Finally, the lack of understanding of information security from the organization staff as a part of the organization culture leads to a loss of confidentiality.

The big challenge is how to face the SE, and to keep up on professionality to mitigate attacks effect, that can be achieved by increasing user awareness at first, through education programs for different ages, be-cause they are the weakest link in the security system [19,4,7]. The governments should enact laws to protect citizens as in Australia, then the author listed some techniques for next-generation based on gam-ing, video, and simulation methods for phishing as an example [19,7]. On the other hand, earlier training in cybersecurity for students will minimize the number of victims in the future [4]. Keeping the operating system, protection, and security programs up-to-date will also reduce the SE effect [7].

Parthy et al. [6] and Lekati [22] Recommends using behavioral reverse engineering to face SE attacks, which defined as an art science that traces back the process of attack to know how the attackers think and apply their attacks, thus, the tracer can find the locations where the attack starts.

The qualitative study [18] tried to find a secure environment with trusted solutions and good mitigation tools for SE attacks, it proposes that the increase in knowledge of SE attacks leads to a decrease in their success, or to be as a victim of SE, and share with the experts their experiences and skills to gain the best practical ways to protect against SE.

Bhusal et al. [20] confirms the government responsibility to train citizens to deal with private information and to keep them secure from information collectors, this is done co-operatively with the service provider contributes by education, training and awareness program (ETA), additionally using prevention, and detection tools and suitable education are necessary to deal with SE attacks especially the individual training because most of organizations try to rehabilitate their employees to stay away from threats and mitigate loss after attacks, finally, the study summarizes list of countermeasures depending on human interaction(direct, indirect) to stop existing attacks like avoiding logging in suspicious sites, using strong and complex password, using two-factor authentication, as indirect human interaction, giving confidential in-formation via phone or email about your accounts or passwords, and avoid dealing with emergency email/SMS such as "you win in lottery" or "pay immediately" etc. as direct human interaction.

4. Discussion

Studies used different concepts to express SE attack frameworks, i.e., lifecycle, phases, framework, tem-plate, and model, which becomes more important over time as the average of cybercrime gets high. Most studies agree on the effect of a clear and inclusive framework to understand, face SE attacks, and the effect on awareness. Findings in studies highlighted different bases to construct or develop SE attack frameworks, such as attack base which depend on technical taxonomy, for example, types of attack, and human base which depends on non-technical taxonomy and

focuses on psychology, e.g., human vulnerabilities and effects in details, on the other hand, there are some studies concentrate on attacker mechanisms, others concentrate on details of each phase and the flow of connection between each part of the framework.

All studies' results express the need for more empirical studies, financial support, and government per-mission to face SE attacks, and approve their conceptual frameworks and apply those frameworks in various cultures, that contain an inclusive share of societies with different factors e.g., educational level, awareness level, age, gender, and culture. That means the connection becomes clearer between the phases of the SE attack.

Furthermore, the researchers can examine their proposed frames and match the efficiency and test them in a number of scenarios. Therefore, the security manager can access and implement the model of frame-work easily and cover all attack entities, and so decreases the effect of SE attack more quickly than un-comprehensive models or frameworks.

So, in most of the studies, there is a need to add a new phase or entity that contains the defense methods for SE attacks to give an integrated view of the framework, because the attackers have flexibility in their techniques thus, they can develop an attack that depends on the defense strategy the victim has taken, so the process must be continuous and evolving.

Studies which covered awareness objective have many points in common, i.e., agreeing on the im-portance of the level of consciousness, and how does the awareness affect in decreasing SE attacks effect, next points show three levels that play an important role in awareness to face SE attacks, as Table 5 shows:

1) Governmental level which introduces legislations to protect citizens rights from cybercrimes, to deter attackers, develop educational curricula that support security trends in cyberspace to reduce the effect of cybercrimes, demanding service providers to meet security standards, especially confidentiality for customers, and provide financial support to researchers in cybercrime area especially in SE attacks.
2) User-level which depends on awareness of the user and their direct and indirect interaction, to learn and educate self on how to deal with cyberspace to prevent threats, e.g., phishing, and raise up their knowledge in types of cyberattacks, then increase their sense of cybersecurity, finally, embrace im-portance of passwords complexity and the nature of the information they display on public e.g., social media.
3) Organization level which protects employees from being victims of SE attacks and to prevent any fi-nancial losses, or any fraud trials to compromise employees' personal information and use it against them.

Table 5. An important role in awareness to face SE attacks

Level	Sub-level	Responsibility
Government	Legislations	Enact law save citizen rights, and deter the attackers
	Curricular	(ETA) Educational curricula, training programs, and awareness.
	Service providers	ETA and prevention/ detection tools
	Financial support	For the Research, ETA, and defense tools
Individual user	Knowledge	Raised up his sense of cybersecurity by self-educating (ETA)
	Interaction	Direct (don't give password via non-confidential tunnel) Indirect (put a complex password)
Organization	Employees	ETA and use prevention and detection tools
	Customer	ETA; Depending on their needs

5. Conclusion & Future work

This paper is a qualitative SLR which explores previous studies in SE concept, attack framework, aware-ness needs between 2014 to 2021 by analyzing 20 papers that is presented in eligibility criteria, using Pris-ma 2020 methodology. The extracted data shows the need for more studies in all research objectives. For the definition of SE, there is lack in finding clear and related concept to give the exact expression of SE attack in cyberspace. The review surveyed previous studies which proposed different frameworks in differ-ent perspective, cycle, phase, model, and session base, by various factors like psychology weakness, SE methodology, attack mechanisms, attack techniques, and the goals; achieved or not? But there is a need to approve them empirically by applying the researches in larger samples, with inclusive factors to neutralize the bias depending on sample size, that means the need of government cover as resources and financial supports. Moreover, all of results indicates how it is necessary to find a comprehensive conceptual frame-work for SE attacks? how that contribute in rise up defense strategy and the mitigation tools? and the effect on awareness which summarized in three levels of responsibility i.e., government, individual user, and or-ganization, the responsibility divided between them in ETA, but government takes the important part for enact laws, and financial support. These results may be considered as good ideas to start future work.

In future work, the author suggests conducting wide comparative study to build an integrated conceptual framework for each stage of SE attacks, and include the mitigation countermeasures within it.

Author Contributions

Conceptualization, R.A., and D.E.; Methodology, R.A.; Formal Analysis, R.A.; Investigation, R.A.; Re-sources, R.A.; Writing-Original Draft Preparation, R.A.; Writing-Review & Editing, R.A., and R.A.; Visu-alization, R.A.; Supervision, D.R.; Project Administration, D.E.; Funding Acquisition, R.A.

Acknowledgment

R.A wishes to thank Palestine technical university-kadoorie (ptuk) for supporting this research work.

References

[1] "ISACA's State of Cybersecurity 2021, Part 2: Threat Landscape, Security Operations and Cybersecuri-ty Maturity, [Online]. Available: www.isaca.org/state-of-cybersecurity-2021."

[2] "2021. Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends. [Online]. Available: https://purplesec.us/resources/cyber-security-statistics."

[3] "2020. Internet Crime Report. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf Washington, D.C., FBI National Press Office, (202) 324-3691."

[4] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Future Internet, vol. 11, no. 4. MDPI AG, 2019. doi: 10.3390/FI11040089.

[5] C. Sekhar Bhusal, "Systematic Review on Social Engineering: Hacking by Manipulating Humans," Journal of Information Security, vol. 12, no. 01, pp. 104–114, 2021, doi: 10.4236/jis.2021.121005.
[6] 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019.
[7] D. Eleyan, A. Eleyan, and N. A. Odeh, "A SURVEY OF SOCIAL ENGINEERING ATTACKS: DE-TECTION AND PREVENTION TOOLS Software engineering View project The ant lion optimizer (ALO): theories, variants, and applications View project A SURVEY OF SOCIAL ENGINEERING ATTACKS: DETECTION AND PREVENTION TOOLS," Journal of Theoretical and Applied Infor-mation Technology, vol. 99, no. 18, 2021, [Online]. Available: https://www.researchgate.net/publication/355410947
[8] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic re-views," BMJ, vol. 372, 2021, doi: 10.1136/bmj.n71.
[9] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "IFIP AICT 431 - Towards an Ontological Mod-el Defining the Social Engineering Domain," 2014.
[10] Z. Wang, L. Sun, and H. Zhu, "Defining Social Engineering in Cybersecurity," IEEE Access, vol. 8, pp. 85094–85115, 2020, doi: 10.1109/ACCESS.2020.2992807.
[11] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vul-nerabilities and attack methods," IEEE Access, vol. 9, pp. 11895–11910, 2021, doi: 10.1109/ACCESS.2021.3051633.
[12] L. Karadsheh, H. Alryalat, J. Alqatawna, S. F. Alhawari, and M. A. al Jarrah, "The impact of social engineer attack phases on improved security countermeasures: Social engineer involvement as mediat-ing variable," International Journal of Digital Crime and Forensics, vol. 14, no. 1, pp. 1–26, Jan. 2022, doi: 10.4018/IJDCF.286762.
[13] H. S. Venter and Institute of Electrical and Electronics Engineers, 2014 Information Security for South Africa: proceedings of the ISSA 2014 Conference: 13-14 August 2014: Radisson Blu Gautrain Hotel, Sandton, Johannesburg, South Africa.
[14] F. Mouton, L. Leenen, and H. S. Venter, "Social Engineering Attack Examples, Templates and Sce-narios." [Online]. Available: http://www.social-engineer.co.za/
[15] A. Yasin, R. Fatima, L. Liu, J. Wang, R. Ali, and Z. Wei, "Understanding and deciphering of social engineering attack scenarios," Security and Privacy, vol. 4, no. 4, Jul. 2021, doi: 10.1002/spy2.161.
[16] K. Zheng, T. Wu, X. Wang, B. Wu, and C. Wu, "A Session and Dialogue-Based Social Engineering Framework," IEEE Access, vol. 7, pp. 67781–67794, 2019, doi: 10.1109/ACCESS.2019.2919150.
[17] A. H. Washo, "An interdisciplinary view of social engineering: A call to action for research," Com-puters in Human Behavior Reports, vol. 4, p. 100126, Aug. 2021, doi: 10.1016/j.chbr.2021.100126.
[18] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues," Future Internet, vol. 11, no. 3. MDPI AG, 2019. doi: 10.3390/fi11030073.
[19] IEEE Staff, 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engi-neering (TALE). IEEE, 2018.
[20] C. Sekhar Bhusal, "Systematic Review on Social Engineering: Hacking by Manipulating Humans," Journal of Information Security, vol. 12, no. 01, pp. 104–114, 2021, doi: 10.4236/jis.2021.121005.
[21] H. Aldawood and G. Skinner, "Analysis and Findings of Social Engineering Industry Experts Ex-plorative Interviews: Perspectives on Measures, Tools, and Solutions," IEEE Access, vol. 8, pp. 67321–67329, 2020, doi: 10.1109/ACCESS.2020.2983280.
[22] C. Lekati, "Complexities in Investigating Cases of Social Engineering: How Reverse Engineering and Profiling can Assist in the Collection of Evidence," in Proceedings - 11th International Conference on IT Security Incident Management and IT Forensics, IMF 2018, Oct. 2018, pp. 107–109. doi: 10.1109/IMF.2018.00015.
[23] K. D. Mitnick, W. L. Simon, and S. Wozniak, The art of deception: controlling the human element of security. Wiley Publishing, 2002.

RUWA' F. ABU HWEIDI received the B.S. degree in computer science from the An-Najah University Nablus, Palestine. She is also pursuing an M.S. degree in cybercrimes and digital evi-dence analysis in Palestine Technical University-Kadoorie (PTUK), Tulkarm, Palestine, she worked as a teacher and computer lab instructor from 2004 to 2018 in ministry of education, before retiring from in 2018.

DERAR ELEYAN is Associate Professor, Palestine Technical University- Kadoorie, De-partment of Applied Computing Tulkarm, Palestine. PGDE (Professional Graduate Diploma of Education for Teaching Further and Higher Education). Bolton University, Graduated date June 2008. - PGC Engi-neering Management, Bolton University, July 2007-September 2007. PhD, in Information Systems Engi-neering, University of Manchester, October 2006. It is about building a system dynamics model to serve as a solution-directed model for project management review using Earned Value Management System. MSc, Business Information Technology, South Bank University, London, 2002/2003. BSc, Computer Science, Amman University, 1994.