IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 7, 2022, accepted March 17, 2022, date of publication March 28, 2022, date of current version April 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3162594

Social Engineering Attacks Prevention: A Systematic Literature Review

WENNI SYAFITRI[1], ZARINA SHUKUR[1], UMI ASMA' MOKHTAR[1], ROSSILAWATI SULAIMAN[1], AND MUHAMMAD AZWAN IBRAHIM[2]

[1]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor 43600, Malaysia
[2]National Metrology Institute of Malaysia, Bandar Baru Salak Tinggi, Sepang, Selangor 43900, Malaysia

Corresponding authors: Wenni Syafitri (wenni20@gmail.com) and Zarina Shukur (zarinashukur@ukm.edu.my)

This work was supported in part by the Malaysia Ministry of Education under Grant KKP 2020/UKM-UKM/4/3, and in part by the Department of Commerce under Grant BS123456.

ABSTRACT Social engineering is an attack on information security for accessing systems or networks. Social engineering attacks occur when victims do not recognize methods, models, and frameworks to prevent them. The current research explains user studies, constructs, evaluation, concepts, frameworks, models, and methods to prevent social engineering attacks. Unfortunately, there is no specific previous research on preventing social engineering attacks that effectively and systematically analyze it. Current prevention methods, models, and frameworks of social engineering attacks include health campaigns, human as security sensor frameworks, user-centric frameworks, and user vulnerability models. The human as a security sensor framework needs guidance that will explore cybersecurity as super-recognizers, likely policing act for a secure system. This paper intends to critically and rigorously review prior literature on the prevention methods, models, and frameworks of social engineering attacks. We conducted a systematic literature review based on Bryman & Bell's literature review method. We found a new approach in addition to methods, frameworks, models and evaluations to prevent social engineering attacks based on our review, which is using a protocol. We found the protocol to effectively prevent social engineering attacks, such as health campaigns, the vulnerability of social engineering victims, and co-utile protocol, which can manage information sharing on a social network. We present this systematic literature review to recommend ways to prevent social engineering attacks.

INDEX TERMS Social engineering attacks prevention, systematic literature review.

I. INTRODUCTION

Social engineering attacks manipulate victims by attacking the weakest link. Social engineering requires that a victim stands in an asymmetric knowledge-relation to the attacker, who uses this asymmetry to establish technocratic control over the victim [1]. Technocrats are people with a skill or specific technical knowledge such as dentistry or economic planning. Asymmetric knowledge occurs when people or groups have more significant satisfaction and knowledge than other people in the specific knowledge area. Hatfield [1] elaborates on social engineering attacks from 1842 until the current cyber age. This paper has limited use because it only explained the evolution theory of social engineering.

A social engineering attacker is a person who wants access to sensitive information or money. The attacker will cause discomfort to bypass, notifying the victim's vengeful objective when was manipulating the victim. Based on The National Institute of Standards and Technology (NIST), social engineering is an attempt to trick someone into revealing information (e.g., a password) to attack systems or networks [2]. Successful social engineering attacks depend on a target being manipulated or tricked into disclosing personal information [3].

Social engineering attacks have evolved into telephone calls, emails, and face-to-face interactions. Social engineering attack methods consist of impersonation, social engineering attacks on an online community or social media, automated social engineering, and semantic attacks. Various types of social engineering are developing along with the spreading of information technology. Previous

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

research on human manipulation has been found that perpetrators manipulated or tricked employees psychologically, for instance, using social engineering and phishing attacks, into committing security mistakes or giving away sensitive information [4]. Verizon's Data Breach Investigation Report explained the top incidents consist of phishing and pretexting [5]. Two of these types of attacks are social engineering attacks; therefore, social engineering attacks remain active until they obtain victims. Another types of social engineering attack can be found in online interaction such as online scams [6], [7], cyberbullying, sharing disadvantages image/text, privacy communication [8] and non-financial disclosure aspect [9].

Social engineering attacks prevention methods are health campaign strategies, health campaign tactics, television advertisements, informational pamphlets, social media [10], ethics of social engineering penetration testing [11], a human as a security sensor framework [12], a personality information processing model [13], characteristic user framework [14], Game-based analysis [15], and predicting individuals' vulnerability [16], computer security policy [17], cyber security practices [18].

Another study explained privacy and security [19]–[23]. Topic research about behavioral aspects of cybersecurity were proposed in [24] and [25]. The latest research about the Sybil attack on social networks could be viewed in [26].

This literature review presented current solutions for attacks, such as health campaigns that could prevent social engineering attacks, especially psychological effects of different techniques and general knowledge of social engineering attacks [10]. However, there were no explanations of the results in this previous research. Penetration testing can protect against social engineering attacks, but it should not only be considered a partial analysis of the broader ethics of social engineering in cyber operations [11]. A human as a security sensor framework can be one of the most vital links for detecting deception-based threats; furthermore, a direction for research may be to explore whether cybersecurity can benefit as "super-recognizers" in the same way policing does [12].

Perceptions of risk and precautionary behavior models can help users avoid methodological fallacies. The literature included recommendations for behavioral interventions to improve security and privacy among Facebook users. Future research should consider this issue as a predictor of perceived risk and precautionary behavior [19].

The problem with this research that steps of prevention social engineering attacks will protect users. There is not a solution that related to Sánchez's research for the detection of malicious information. The solution for this problem is a systematic literature review of methods and frameworks for preventing social engineering attacks and finding malicious information practically. The literature included in this review was published between 2018 and 2021. The research overview can be viewed in Fig. 1.

This literature review is structured as follows. Section II explains the systematic literature review for the prevention of social engineering attacks. Section III describes the methodology. Section IV explains the results of this systematic literature review. Section V presents the conclusions of this paper.

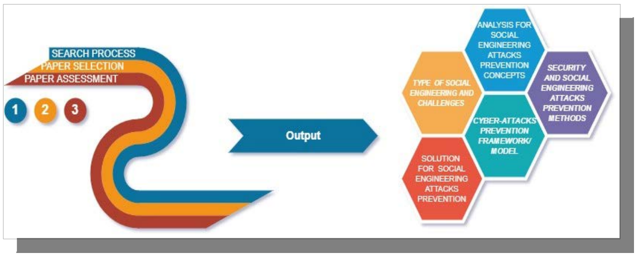
SEARCH PROCESS
PAPER SELECTION
PAPER ASSESSMENT
1
2
3
Output
TYPE OF SOCIAL ENGINEERING AND CHALLENGES
ANALYSIS FOR SOCIAL ENGINEERING ATTACKS PREVENTION CONCEPTS
SECURITY AND SOCIAL ENGINEERING ATTACKS PREVENTION METHODS
CYBER-ATTACKS PREVENTION FRAMEWORK/ MODEL
SOLUTION FOR SOCIAL ENGINEERING ATTACKS PREVENTION

FIGURE 1. Research Overview.

II. RELATED RESEARCH

Very few researchers have reviewed the prevention of social engineering attacks. At the same time, social engineering techniques are hazardous and can create catastrophic losses for the organization.

Hijji and Alam reviewed social engineering attacks during the Covid-19 pandemic using the Multivocal Literature Review (MLR) technique. Hijji and Alam reviewed the techniques, attacks, and platforms used during the Covid-19 pandemic [27]. MLR collaborates between research results and perspectives from practitioners. The MLR conducted by Hijji and Alam has weaknesses in terms of discussion, such as source criteria from a practitioner's perspective and research results that are not explained in more detail. Hijji and Alam stated that a practitioner's perspective criteria are reputable reports, blogs, websites, whitepapers, and magazines. As for the research results, only Google search, Google Scholar and Scopus.

Bulle and Junger reviewed social engineering attacks by investigating interventions to reduce the impact of social engineering attacks. Meta-analysis was used to perform the review. The meta-analysis combines review results and statistical techniques to summarize research results quantitatively. The criteria for the articles reviewed are to have and test experimental designs built to reduce the vulnerability of social engineering attacks. The limitation of the research found by Bulle and Junger is that the article is limited to countries with the category of Western, Educated, Industrialized, Rich, and Democratic (WEIRD) [28]. Another limitation of Bulle and Junger is that the intervention was not found due to more specific research criteria, so that the purpose of the investigation has not been fully achieved.

Schab *et al.* conduct a review of the defense strategy against social engineering attacks [29]. The literature used by Schaab *et al.* takes the perspective of information technology security practitioners and social psychology. Schab *et al.* divided the articles found into social psychology groups such as Authority, Social Proof, Liking, Similarity, Deception, Commitment, Reciprocation, Consistency, and Distraction.

TABLE 1. Comparison of review articles related to the research conducted.

Source	TYPES	Challenge	Prevention Type	Prevention Aspects	Prevention Approach
[27]	√	√			
[28]	√	√			
[29]		√	√		
[30]	√	√	√		
[15]	√				
[31]	√	√			
[32]	√	√			
This Survey	√	√	√	√	√

However, Schaab *et al.* did not conduct a more comprehensive review, and this was because it did not use the literature review methodology used, such as Hijji and Alam. The social engineering attack defense strategy was carried out by Schaab *et al.* limited to prevention from social psychology.

Yasin *et al.* review social engineering in two categories, namely the type of attack and the persuasion technique used [15]. Yasin *et al.* also combine several theories to explain how social engineering attack activities are carried out. However, Yasin *et al.* did not provide how the prevention techniques should be carried out by users against the types of attacks and persuasion techniques used by social engineering attacks. So the research conducted by Schaab *et al.* is better than Yasin *et al.* in terms of technical recommendations for preventing social engineering attacks.

Salahdine and Kaabouch conducted a social engineering review in four categories: attacks, classification, detection strategies, and prevention procedures [30]. The review technique used by Salahdine and Kaabouch is the same as that used by Schaab *et al.*, only dividing the review into several categories. However, what distinguishes the study of Schaab *et al.* is to make comparisons against attacks and social engineering attack prevention techniques from a technical and human perspective. The advantages and disadvantages of social engineering attack prevention techniques are briefly described.

Wang *et al.* [31] and Wang *et al.* [32] reviewed the types and challenges of social engineering. the results of a review conducted by Wang *et al.* [31] was able to define the true meaning of social engineering activities in cybersecurity. The review conducted by Wang *et al.* [31] is very systematic and the use of advantages and disadvantages analysis is used to compare the existing theories. Wang *et al.* [31] and Wang *et al.* [32] did not review the known prevention of social engineering attacks, this is because Wang *et al.* [31] wanted to clarify the boundaries and where social engineering activities are located. While Wang *et al.* [32] only focuses on the mechanism of effect and human vulnerability to social engineering attacks by being proven by 16 scenarios to prove how it is applied. Research development recommendations Wang *et al.* [32] which is to prove the factors that can detect the vulnerability of social engineering attacks.

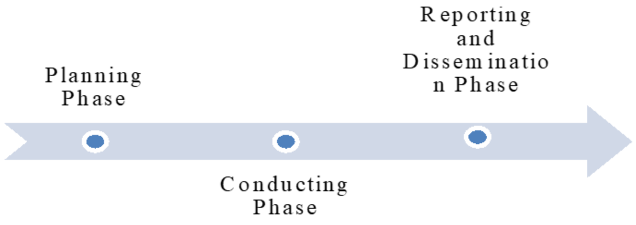

FIGURE 2. Systematic literature review phase.

This research focused on the model/framework for preventing social engineering and social media attacks and ensuring privacy on social media. Therefore, selecting a systematic literature review technique is appropriate because it relies on good quality scientific articles [27]. However, there is no systematic literature review to the best of our knowledge to prevent social engineering attacks; thus, this paper closes the gap.

III. METHODOLOGY

A. RESEARCH METHODS

This systematic literature review is conducted based on [33]. These review methods about prevention of social engineering attacks are developed in this systematic literature review. The literature review process is shown in Fig. 2. There are three phases of systematic literature review: planning, conducting, and reporting. The planning phase determines the research question and makes it clear and answerable.

B. SEARCH PROCESS

Searching criteria, paper selection, and paper assessment define the literature review process. This systematic literature reviews searched papers using four digital databases, used search strings to gather several papers, and selected relevant papers based on year, article type, and title. Databases on this research used four digital databases, such as Elsevier, IEEE, Springer, and Willey.

The research question is the necessary factor of a systematic literature review. The research question focused on the research method, framework, and model of prevention of social engineering attacks.

Research Question: "Which is the most effective method, framework, and model for the prevention of social engineering attacks?"

This systematic literature review aims to find, analyze, and summarize prevention methods and frameworks/models of social engineering attacks.

Searching criteria of this literature review are related to the keyword "Prevention Social Engineering Attacks." Search string on this systematic literature review: (Prevent∗) AND (Social Engineering Attacks).

C. PAPER SELECTION

An excellent systematic literature review must have review criteria. The nearest context identified paper selection on the research objective. The paper selection criteria are

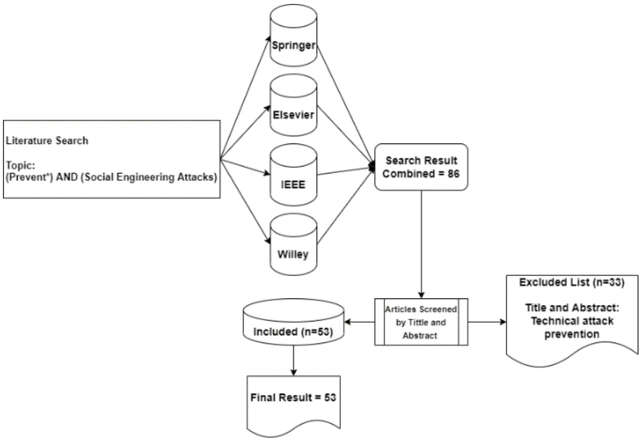

FIGURE 3. Paper selection process.

related to keyword, topic, publication year, and journal publisher which have related in ''Prevention Social Engineering Attacks''. There are sixteen Elsevier databases, twenty seven papers from IEEE databases, seven papers from the Springer database, and three papers from Wiley database papers.

D. PAPER ASSESSMENT

After paper selection, the next step is paper assessment. Paper assessment is a way to get an appropriate paper that execute based on research context and criteria. A matrix conducted in this paper assessment has many information criteria, such as title, author, year, keyword, publisher, Q category, methods, main contribution, advantages, limitation, the definition of social engineering attacks, and prevention methods/models/frameworks for social engineering attacks.

A schematic information area constructs the next step that is known as the paper assessment:

(1) Analysis concept of prevention of social engineering attacks
(2) Prevention methods of security and social engineering attacks
(3) Prevention models/frameworks of security and social engineering attacks

The result of the paper assessment will be explained in the following section.

IV. RESULT

A. TYPE OF SOCIAL ENGINEERING AND CHALLENGES

Social engineering is an attack that can avoid all hardware or software that serves to prevent attacks in general. Social engineering is challenging to prevent if it relies on hardware or software technology. This is caused by social engineering attacks attacking users who use technology from both hardware and software. Therefore the prevention of social engineering attacks must involve the device's user. Social engineering attacks are very diverse and often change depending on the use of the technique. The following explains the various types of attacks and the challenges of social engineering attacks.

1) PHISHING

Hackers send messages that have been modified so that users believe that the messages received are legitimate, and users are required to follow the instructions or suggestions in the message. The most widely used examples of phishing are email and website phishing. Some phishing uses malware, bots, and trojans to gain more users access [27].

Vishing is a part of phishing that focuses on communication lines using telephone media. Hackers use Vishing to direct users to provide confidential information, such as PINs, One-Time-Passwords, and the like, without the user realizing it. Hackers use several psychological techniques, such as giving threats, anxiety or good news so that victims do not realize they are not being scammed. Examples of Vishing often used are Impersonation on Help Desk attacks (IHD) and Robocall [30]. IHD attacks exploit help desk employees to obtain specific information or services by pretending to be the most influential people in the organization. Robocall attack combines Voice over Internet Protocol (VoIP) and text to speech technology to exploit the weakness of users who have publicly known telephone or VoIP numbers. More specific targets are mobile phones, fixed-line telephones, and office telephones. These robocalls usually carry out the attack mode by offering services or products and even solving a problem.

Apart from Vishing, phishing attacks focus on sending messages using SMS technology, namely Smishing. The way smishing works are almost the same as email phishing attacks. Hackers send messages to users containing vital information or must be followed up immediately using SMS to phone numbers that can be known publicly or randomly. This Smishing attack is perilous because it is more personal, making the victim less alert.

Spearphishing is a phishing attack that can be an attack that hackers target. This attack is almost the same as a Whaling attack, namely a phishing attack that targets the leader or the most influential person in the organization. If Spearphishing with the Whaling concept is used, the impact on the organization will be very detrimental.

Another type of phishing attack is Pharming, where hackers divert user transaction traffic on a website to a fake website to take information or money. Man-in-the-middle-attack is an attack that is almost the same concept that is carried out; only the difference in the media used to use phishing is email messages. Modification is done when an email exchange between the recipient and the sender uses a Trojan horse [34].

One of the new phishing techniques is Angler phishing, in which hackers clone profiles on a company's customer service account on social media to attack the company's customers. The most priority targets for this attack are customers who have disappointment or pleasure in the services of a company or organization. These customers can be targeted by Angler phishing attacks based on their social media status, expressing disappointment or pleasure. Hackers take advantage of this attack to get credentials or personal information.

2) GROOMING

One of the newest social engineering techniques is Grooming, which uses psychological techniques and information technology to obtain confidential information related to potential victims of pedophilia. Grooming techniques focus on using information technology such as SMS, email, and telephone. The conversation is more of a trap to become a victim of pedophilia [35].

3) PRETEXTING

Hackers get public information sourced from websites, social media, and telephone books to link information about an activity in which the victim has been involved or has the opportunity to be involved in the activity. Pretexting is a phishing technique that relies on two-way communication; there is a conversation with the victim. Conversations can take the form of offering work or help, asking for personal information or confirming getting a prize [30].

4) PROFILE CLONING

This technique utilizes publicly available information, such as social media, to act like someone whose profile is cloned to get important information from other people [36], [37]. Public information can be in images, videos, full names, and even conversational styles sourced from social media. If the hacker wants to get information from the victim, the hacker will try to find a way to provide the information needed by the hacker. Hackers can use the IHD concept, namely looking for people who have more influence on the victim, for example, ''B.'' Hackers use the Profile Cloning technique on ''B'' then start contacting the victim to get confidential information using several indirect social engineering techniques such as Phishing or Pretexting.

5) FACE-TO-FACE INTERACTION

Social engineers commonly use this technique; namely, social engineers meet face-to-face by taking advantage of the victim's psychological weaknesses such as helping then seducing or begging to get physical access or not to information [6].

6) SHOULDER SURFING

However, this technique is very commonly done by people who do not have social engineering skills. This technique takes advantage of human nature, unaware of the surrounding conditions when interacting with access or essential information. An example is when someone is using a laptop or computer to access a confidential information system, where someone behind it is not interested in the system [30].

7) QUID PRO QUO ATTACKS

Quid Pro Quo is an attack that expects reciprocity from a free service or product [30]. This social engineering attack concept adopts ''There Is No Free Lunch.'' This attack requires an agreement between the victim and the hacker, such as the victim asking the hacker to do something beyond the victim's ability, and then in return, the victim must submit important information or something else in exchange for a favor.

8) DUMPSTER DIVING ATTACKS

This attack takes advantage of human weaknesses who fail to filter out information or documents in the form of physical or non-physical that is no longer used. Documents or information thrown into a landfill or deleted a folder or file on the hard drive will be valuable information for data collectors from Dumpster Diving attacks [30].

9) DIVERSION THEFT ATTACKS

This attack uses courier companies to insert malware or rootkits into computers or systems sent and used by a company [30]. So that product installed malware or rootkits is not detected and enters the company network.

10) PIGGYBACKING OR TAILGATING OR TRAILING & PRETENDING

Piggybacking or Tailgating or Trailing & Pretending attacks exploit the power of organizational members to access certain information. Hackers only need to follow activities escorted by members of the organization, so hackers can freely pass through the security perimeter within the organization [15], [31], [32].

11) FILE MASQUERADE

This attack occurs when users are unaware of every file on their computer or external storage media. Users feel confident that the computer or storage media is free from malware or trojans. Malware or trojans have been inserted into user files so that when users see files that are usually opened, there is no hesitation from the user to execute the file [15].

12) BAITING

This technique uses a simple method by utilizing members of the organization who have a high curiosity about something. The concept is that hackers use electronic media in physical form to attack organizations, such as USB drives that have been infected with malware or trojans [38].

13) REVERSE SOCIAL ENGINEERING

Hackers create conditions where the victim will fall into the Reverse Social Engineering trap. Hackers make victims of fundamental problems in the organization. Then hackers come to victims directly or indirectly to offer help [38]. For example, they were making the system not work when the victim wants to access it, then offering assistance to fix the system to function as it should so that hackers can freely install any program that can be used to take administrative access through the victim's computer.

14) SCAREWARE OR POP-UP WINDOWS

This attack uses pop-ups on windows or browsers that appear when a user performs an activity, such as accessing a site or the internet suddenly down. Certain web pages have been inserted scripts or codes that can generate pop-ups that can be adjusted to target victims, such as flashing colors or scary sounds. Pop-up models can be in the form of information to immediately click on the user, such as a virus that enters the user's computer or advertisements that can attract users [30].

15) WATER-HOLING

Websites that have a high traffic rate are hacked and then embed malware or trojans on the website. The Water-holing technique only waits for the user to click on the link or download the application on the hacked website so that there will be two-way communication between the hacker and the victim [31].

B. ANALYSIS CONCEPT OF PREVENTION FOR SOCIAL ENGINEERING ATTACKS

Hatfield's research presents the concept of social engineering attacks; it states that the best way to prevent them is to educate and train potential victims [1]. Accordingly, victims must have sufficient knowledge to defend against social engineering attacks. Deploying a health campaign is one of the prevention strategies for social engineering attacks. Identifying a social engineering attack as a semantic attack is challenging because of the behavioral deception that technical defenses cannot detect [12]. In Heartfield & Loukas research [12], there is a combination of technical and behavioral defense; thus, it prevents, detects, and reports semantic social engineering attacks. Additionally, it needs super-recognizers, human sensors that can analyze suspects over surveillance footage.

Research on behavioral against social engineering attacks has been studied thoroughly by [14], [16]. They proposed a user-centric framework [14] and a prediction approach of an individual's vulnerability [16]. The user-centric framework is based on four constructs: social-psychological, socio-emotional, perceptual, and habitual. This framework advantages appraise and figures out the employee perspective of using social networks to control trigger prevention mechanisms, especially education-based prevention mechanisms. Furthermore, establish empirical testing of the factors and dimensions of social engineering that suggested a user-centric framework.

Research on predicting individuals' vulnerability adopts a scenario-based experiment to investigate the correlation between behavioral constructs in the model's ability and conceptual model to anticipate social engineering victims' vulnerability [16]. This research has three angles—the behavior of people, perception, and socio emotions. The angle, behavior of people, is measured with three factors—level involvement, number of social network connections, and social network experience on awareness of social engineering in the conceptual model. Perception angle, which influences awareness of social engineering attacks, has three subfactors—risk perception of people, competence, and cybercrime experience. The socio-emotional perspective will trigger the risky behavior of potential users with two subfactors: trust and motivation. The resulting research positively affects the user's perceived risk within the cybercrime experience subfactor, which is the most determinant trust of people in disclosing private information on a social network. People's motivation affects user involvement, trust, and previous experience with cybercrime. The research limitations were unavoidable due to ethical considerations; some people were unaware that social engineering victims and experiments focused only on academic communities.

Abe & Soltys [10] proposed health campaign strategies and tactics against social engineering attacks, such as television advertisements, physical information pamphlets, and social media discussions. However, this campaign strategy and tactics must have a proper and adequate education. Another limitation of this research was qualitative research, which did not have empirical testing.

Das Gupta *et al.* [20], Sánchez *et al.* [21], and Van Schaik *et al.* [19] proposed the prevention of privacy and security attacks. Identifying and assessing privacy violations of attacks onboard networks, which are theoretical, empirical, and quantified, is presented by Das Gupta *et al.* [20]. This research examines a new and substantial private appraisal for social networks to protect a social network against privacy attacks. On the other side, co-utile protocols were a protocol to protect information disclosure on social networks [21]. This protocol aims to assess data such as an attribute value, a tag, and part of a message and to assess privacy risk based on the data semantic. This research has built self-accomplishment of exchange information and user privacy awareness.

Additionally, future research must expand to identify malicious behavior and give punishment based on reputation. In other research, Van Schaik *et al.* [13] used risk perception and precautionary behavior factors. This correlated research variation between hazards in risk perceptions of people with security and privacy on social networks and determined predictors of perceived risks and precautionary behavior in Facebook use concerning risk perception and security. Furthermore, this research must build insight, especially the protection motivation theory, when applied to security and privacy.

TABLE 2. Prevention social engineering attacks keyword.

Prevention of social engineering attacks	Social engineering attacks	Privacy and security attacks	Social network / social media attacks
References	[10] [16] [14] [11] [12]	[20] [21] [19]	[26] [13] [25]

TABLE 3. Prevention methods of security and social engineering attacks.

N o.	Research Method	Research Type	Attack/ Security Category	Author
1	Prevention of social engineering strategies	Qualitative Research	Social engineering attacks	[10]
2	Assess privacy factor	Quantitative Research	Privacy	[20]

There are three research studied by [13], [25], [26] on social networks or social media attacks. Asadian & Javadi [26] proposed a rational user interaction framework that identifies attacks based on distinct social networks and user interaction. This framework considers four steps: (1) convert the graph of the social network, (2) a process converts undirected unweighted graphs into undirect weighted graphs, (3) captures user interactions to categorize toward similar characteristics communities, and (4) uses the modified depth-first search (DFS) algorithm to determine community nature. This research is independent of the user interaction framework from the social network situation. The personality information processing model is a theoretical model to approach phishing awareness on social networks [13]. This model evaluates the related effect of the big five personality model and the heuristic-systematic model of information processing. The five personality traits consist of conscientiousness, openness to experience, extraversion, neuroticism, and agreeableness. This research explained that 17% of the respondents had been phishing victims and established the relationship between gender and personal traits. The heuristic-systematic model of information processing is a relevant theoretical framework of perceptive phishing victims. This research model explained conscientiousness and extraversion, personality traits correlated with the heuristic-systematic information processing model.

Moreover, this research did not analyze specific persuasion strategies, which affected phishing. The various methods of detecting online social network accounts are explained by P. Velayudhan & Somasundaram [25], such as text mining-based approaches, cross platform-based approaches, behavioral profile-based approaches, and behavioral modeling-based approaches. Furthermore, this research needs more advanced technology to detect social network attacks appropriately.

C. PREVENTION METHODS FOR SECURITY AND SOCIAL ENGINEERING ATTACKS

There are three kinds of security attacks prevention, such as social engineering attacks prevention, privacy and security attacks prevention, and human behavior research. A paper on prevention social engineering attack methods [10] and discusses privacy measures [20]. The first method that could prevent social engineering attacks is qualitative research, and the second method that explain about privacy is quantitative research. Table 3 shows the prevention methods for security and social engineering attacks.

TABLE 4. Frameworks/models of prevention cyber-attacks.

No.	Research Framework/ Model	Research Type	Security/ Attacks Category	Author
1	Co-utile disclosure protocol	Quantitative Research	Information Exchange	[21]
2	Personality information processing model	Quantitative Research	Information Processing	[13]
3	User-centric of preventing social engineering attacks framework	Quantitative Research	Social engineering attacks	[14]
4	Human as a security sensor framework	Quantitative Research	Social Engineering attacks	[12]
5	Security and privacy in an online social networking model	Quantitative Research	Security and privacy	[19]
6	User vulnerability to the social engineering model	Quantitative Research	Social engineering attacks	[16]
7	User interactions framework	Qualitative Research	User Interactions	[26]

D. FRAMEWORKS / MODELS FOR CYBER-ATTACKS PREVENTION

The framework of cyber-attacks prevention has been found in this research, such as a user-centric framework to prevent social engineering attacks [14], a human as security sensor framework [12], and a user interaction framework [26]. The prevention model of cyberattacks consists of the personality information processing model [13], the security and privacy in the online social networking model [19], and the user vulnerability to the social engineering model [16].

E. SOLUTION FOR SOCIAL ENGINEERING ATTACKS PREVENTION

This solution for social engineering attacks prevention has thirteen categories. Its categories are based on research written by [39]. The review of this solution could be viewed on the bellow sentences:

1) SOCIAL ENGINEERING POLICY

Khidzir *et al.* [40] Establish management policies for social engineering prevention at four levels. At level one, risk management is carried out against social engineering attacks. At level two, the responsibilities and procedures for carrying them out are described. There is a list of evaluations for preventing social engineering attacks at level three, complete with instructions on how an activity is expressly said to have been completed. At level four, there is a framework that can be implemented into the system to prevent social engineering attacks and is able to accommodate digital evidence of social engineering attacks. Research Khidzir *et al.* [40] further development is needed in terms of how each level of policy management is validated.

Aldawood and Skinner found that human error in implementing policies becomes a challenge for organizations implementing cybersecurity policies, especially against social engineering attacks [41]. One of the reasons is that the policies that have been built have no clear instructions when a social engineering attack occurs or how to prevent it. This is understandable because these social engineering attacks cannot be prevented by using tools but rather by interacting with humans more in terms of education. If forced to monitor every movement of organizational members, it will take time and organizational costs.

2) PREVENTION PROTOCOLS

The prevention protocol, known as the co-utile disclosure of private data, could manage information between social network users [21]. The co-utile protocol calculated social network data privacy risks executed before a privacy functionality score. Before releasing data, the first process calculated the social network's privacy risk, especially types and data structures. In the second process, a privacy functionality score was utility user, which determined social network participation; it summarized the user privacy information study from peers in the social network divided by privacy risk acquired by publishing sensitive information to others. The decentralization of social network interactions, such as a peer-to-peer model, and explicit reciprocity of information disclosure, was used as the co-utile protocol. This research proposed a co-utile protocol that will be resists rational attack because of its mutual rational behavior.

3) USER STUDIES

User Studies of this literature review can viewed in the following papers: [4], [10], [13], [14], [16], [19], [23], [42]–[44]. Albladi & Weir [14] used the influence factors of users' proficiency in threat detection and developing susceptible user profiling. This research used a mixed-method approach from expert reviews to validate the characteristic user framework. This research constructed a quantitative and qualitative study. In the first phase of this research, respondents determined framework factors as user awareness of social engineering attacks on social networks. In the second phase of this research, experts gave some assumptions and recommendations to enhance the characteristic user framework. The results of the two studies were analyzed to measure the relevance framework factor to determine user ability to detect social engineering attacks. Furthermore, this research can expand to add an extra security layer for vulnerable user characteristics. In other research, Albladi & Weir [16] examined user characteristics in social networks by three aspects—user perceptions, behavior, and socio emotions—to determine the factor of user vulnerability to social engineering attacks. This research used three analyzed approaches, such as the Partial Least Square algorithm to arrange standard model estimation, a bootstrapping approach to assess the significance of the structural model relationship, and the blindfolding procedure to appraise the structural model's predictive relevance. The result of this research was socio-emotional, affecting user vulnerability. The limitations of this research were using a scenario-based experiment or not using a real attack study, examined only on the academic community. Not all influencing attributes are used in this research.

The personality information processing model analyzed personality traits of user susceptibility to social network phishing [13]. That factor can affect user behavior, such as openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism. This research used the heuristic-systematic model to understand the phishing attack's victimization. Based on research, the heuristic-systematic model simultaneously encouraged personality traits, especially neuroticism, openness, and agreeableness. This research was not representative of the general public because of the small size of the research sample.

Moreover, this research did not construct a directly real-time response and analyze a specific persuasion strategy. Syed [4] explained the impact of a data breach on enterprise reputation on social media. The research aims to analyze the frame of enterprise reputation threat during a data breach and the emergence of enterprise reputation found in the aftermath of data breach pressure on social media. Research design can be conducted by case description and data collection, determining data breach frame and subframes, data breach responsibility, the definition of emotional behavior, and empirical analysis. Based on this research, there were seven subframes defined by three factors—intentional, accidental, and victim. The theoretical directness of enterprise reputation and threat reputation will be used when the data breach occurred and produced a classification of a data breach in the form of frames and subframes. The limitation of this research was the future research that should expand to another type of business, social network, and crisis to conclude the result. Limit the user's account, information sharing of user's account, and information sharing among users' accounts using social media privacy settings [19]. When users share information on social media, they will have risky security and privacy conditions. This research resulted in a significant variation of hazards in perceived risk, risk knowledge, risk by science, risk dimension, precautionary behavior, and benefit. Future research will be performed with other types by defining different antecedents and consequent risk perceptions of social media. Social network anonymization can increase the protection of user privacy [23]. Algorithms to identify social network anonymization are random walk, random add/delete, K-degree, random switch, and clustering. The data set of Twitter and Facebook impacted to result of the algorithms.

Musuva *et al.* conducted experiments to detect whether users are vulnerable to social engineering attacks, especially phishing attacks [44]. The experiment was conducted at a university in Kenya. Musuva *et al.* sent random phishing emails to users at the university. As many as 31.12% of users are vulnerable to phishing attacks.

Bleiman and Rege conducted an experiment on social engineering, namely pretexting on students at a university [43]. Pretexting is a technique that focuses on interacting with the target by playing a specific role more convincingly. The experiments carried out aim to reveal any confidential information shared when exposed to social engineering attacks. Pretexting experiments succeeded in revealing confidential information from students if the hacker had the same traits as the target or played the role of the imitated character better.

Abe and Soltys [10] adopted a health campaign strategy to prevent social engineering attacks. The campaign contains scenarios that can become social engineering attacks and the resulting threats. The campaign is carried out on advertisements on television, pamphlets, and discussions on social media. Abe and Soltys provide education to the public without knowing the measure of the campaign's success. Therefore, further experiments are needed to test whether the campaign was successful or not, as was done by Musuva *et al.* [44].

Burda *et al.* exploit the human ability to detect social engineering attacks [42]. Burda *et al.* build models for detecting and reporting phishing attacks. Burda *et al.* consider social engineering attack reporting activity an untapped innovation and has opportunities for rapid response and attack prevention. The model developed by Burda *et al.* showed promising results for the case studies used only. So it is necessary to prove it to different organizations, especially in reporting and training on preventing social engineering attacks.

4) FEASIBILITY SOCIAL ENGINEERING ATTACKS CONCEPTS

The social engineering concept is explained in Hatfield research [1], in Yasin research [15] presented theory, type of social engineering attacks, and related persuasion technique for social engineering attacks, Parthy and Rajendran [45] presented phases of social engineering attacks, enterprise infrastructure enterprise threat and attacks, countermeasures based on employee and attacks. Three of these research have a different approach to the concept of social engineering. Hatfield focused on story of the social engineering, another research, Yasin focused on type of social engineering attacks and persuasion technique, then, Parthy and Rajendran focused on countermeasure of social engineering that related to enterprise infrastructure. Social engineering is well known used in political aspects whom politician did with their political activity. In cybersecurity, social engineering training aims to train and educate the weakest link of users. Virtue ethics is an analysis of the ethical manner of habit and behavior determined by or set in a social relationship [11]. Analyze virtue ethics by correlating the ethical theories of a penetration tester. There were two theories of virtue ethics in this research, i.e., Utilitarianism and Kantian deontology. Utilitarianism was a step of ethical measurement based on the resulting outcome, not the actor's motives and other factors. Kantian deontology in Hatfield research [11], demonstrated that human manipulation could decrease human dignity. It explained that universality had been a critical characteristic of rationality, in which the same answer from one person governs to find the same choice.

Moreover, Utilitarianism presented by Hatfield [11] is the practical virtue ethics of the penetration test, which will increase security goals. The ethics of white hat social engineering attacks depend on individual concerns and company triggering penetration tests on large-scale social and public contexts. A social engineer must apply mitigation strategies to decrease damage to social engineering victims when penetration testing is executed. Analysis of penetration testing explained in this research must be advised, particularly social engineering ethics analysis on a cyber operation [15]. The phase of social engineering attacks consists of information gathering, gaining trust, exploitation, and exit [45]. There are three categories of enterprise infrastructure: employee, infrastructure and policies, and the technical part of the enterprise system. The enterprise infrastructure must be on the lookout for resilient enterprise system attackers.

5) SOCIO-TECHNICAL

Maalem's research [24] classified behavioral and reviewed crime theories, perceptions, attitude, intent, profiling, and hacking methods. User negligence not to ignore social engineering attacks will significantly impact the organization. Collaboration between knowledge, technology, and information security awareness is needed. Therefore, improving these areas will help increase preparedness to prevent incidents.

Velayudhan and Somasundaram [25] reviewed social engineering prevention techniques on online social networks. Social engineering detection approaches can be text mining, time profile, statistical, composite behavioral, cross-platform, and behavioral profile, which could detect compromised online social network accounts. An online social network account generates an aim or effect for each approach.

Ferreira[46] used a user habit approach technique to force users to click on ransomware. The habitual approach is in the form of persuasion and habitual characteristics. Therefore, a collaboration between user habits and technical aspects needs to be used to prevent social engineering attacks.

Heartfield *et al.* explored the feasibility of predicting user vulnerability to social engineering attacks [47]. Heartfield *et al.* conducted two experiments to explore the feasibility, i.e., the first experiment was used to identify valuable features. Heartfield *et al.* use signal detection theory to get the first experiment's results. The second experiment was to implement the features found using machine learning techniques.

Banire *et al.* explore the experiences of victims of social engineering attacks by building tools based on Artificial

Intelligence [48]. Victims of social engineering attacks are obtained using the Snowball technique. Snowball technique is a recruitment approach where respondents are asked to assist researchers in identifying other potential respondents. Banire *et al.* carry out two activities, namely (1) asking victims of social engineering attacks to participate in the development of Artificial Intelligence (AI)-based social engineering detection tools; and (2) assessing the use of the tools built using the System Usability Scale (SUS). Banire *et al.* succeeded in building AI-based tools based on SUS. However, if the evaluation only uses SUS, the tools can only be used for specific groups. Therefore, acceptance testing should use more specific techniques to technology acceptance instead of using technology, such as the Technology Acceptance Model (TAM).

6) SUSCEPTIBILITY SOCIAL ENGINEERING MODEL

Frauenstein and Flowerday [13] built a theoretical model used to detect the vulnerability of one of the social engineering attacks, namely phishing on social networks. The theoretical model consists of the Big Five personality and the heuristic-systematic models. The theoretical model that was built managed to find out that careful users have a tiny chance of phishing vulnerability.

Albladi and Weir built a model to predict user vulnerability from social engineering attacks based on user characteristics [16]. User characteristics include interactions in social networks such as habitual perspective, level of involvement, number of connections, social network experience, perception perspective, risk perception, competence, cybercrime experience, socio-emotional perspective, trust, and motivation. Most of the characteristics of users in interacting on social networks influence social engineering attacks.

Alturki *et al.* built a model to identify social engineering attacks on social gaming networks [49]. Social gaming network has become a new phenomenon for young people, so the opportunities for cybercrime are also wide open, especially in social engineering. Based on the research results, the perceived severity of the threat, perceived barriers, perceived benefits, self-efficacy, competition, and cooperation factors influence social engineering attacks.

Algarni *et al.* built a model to detect the vulnerability of Facebook users to social engineering attacks [36]. Algarni *et al.* gave a questionnaire containing a modified Facebook user profile, and then respondents were asked to rate each of the Facebook profiles. Based on the research results, the factors of perceived sincerity, competence, attraction, and worthiness have a significant influence on social engineering attacks.

Abroshan *et al.* evaluate that people who can take risks and their decision-making style can be influenced to become victims of phishing attacks [50]. Respondents were asked to play a risk-taking game and then answer questions related to behavior while playing the game. Abroshan *et al.* also conducted a phishing attack simulation to assess participants' ability to recognize phishing attacks. Abroshan *et al.* recommend using a framework to detect social engineering attacks on various cultures and cultures, primarily focusing on gender and other psychological aspects.

7) PERSONALITY AND BEHAVIORAL PROCESSING

Cai et al. [51] developed a cooperative data sanitization technique to manipulate user profiles and friendships on social networks. This technique prevents social engineering techniques, namely inference attacks that exploit insensitive attributes and social relationships. Data sanitization techniques have succeeded in reducing the accuracy of attackers in retrieving sensitive information from users.

Amato et al. [52] developed a technique to detect human behavior in social networks based on two detection steps. The first step is to use data from social networks about regular habits in interacting on social networks. Then the data is trained using the Markov Chain technique. The second step compares abnormal with abnormal behavior in an activity detection framework. The technique developed by Amato et al. successfully detects an unknown pattern of malicious behavior in these two steps.

8) CONSTRUCT EVALUATION

There are four perspectives in user-centric framework research—socio-psychological, habitual, socio-emotional, and perceptual perspectives [14]. Socio-psychological can be viewed as personal traits that can influence phishing victims. The result of this perspective is the culture that can affect user behavior and decision-making of risk. A habitual perspective can be found by the user's social network habit that can affect the vulnerability to phishing attacks. Eight construct types in this research, such as motivation, trust, cybercrime experience, competence, risk perception, social network experience, number of connections, and involvement levels, could detect the user's vulnerability [16]. Amato [52] proposed user unexplained behavior to detect malicious users of online social networks. This research used a standard form of user interaction to get a role model, then executed compliance for both role models and undetermined user activity. Syed's research [4] defined data breach frames, negative emotions, and responsibility properties analyzed to know about company reputation; afterwards, the data breach occurred. Facebook users' experience perceptions could be defined by predicting precautionary behavior and analyzing the perceived risk of Facebook hazards [19].

Preventive social engineering using construct evaluation can still be developed further. Research development can be in the form of: (1) empirical testing with adjustments to various case studies such as Internet-of-Things or cloud computing [14], (2) exploratory focus on the construct of trust in user competence in social engineering attacks [16], (3) further investigation of malicious behaviour against unexplained activity [52], (4) evaluation of constructs to determine the impact of online reputation management on published company ratings [4], and (5) evaluation of risk perception constructs on prudent behaviour [19].

TABLE 5. The concepts of social engineering.

Concept of Social Engineering			Explanation		
Categories	Sub-Categories		Year	Term / Fundamental Ideas	Sub-term
Social engineering evolution by Hatfield [1]	a	Political antecedents	1914	Term "social engineering"	
			1929	Applied social scientists.	
			1938	Describe of conquering Nyasaland.	
			1842	Three fundamental ideas.	Epistemic asymmetry. Technocratic dominance. Teological replacement.
			1940–1960's	Social and Political planning.	History analysis. Religion sociology. Mass movements on social perspective. Concepts of race on anthropology view. Philosophy of political Part of family counseling aspects Factory and laboratory management Agriculture policy history Space exploration analyses Philosophy of social science Jurisprudence on sociological perspectives Technology application Social practices and social science Race in the workplace analyses
			1969	Nobel Prize for Economic Sciences. (Jan Tinbergen from Netherlands and Ragnar Frisch from Norway)	Social policy age explanation by conducted actual application
			early 1970's	Technology Issues	Telephone system
			1970	Daily lexicon of commentators and researchers	
			Middle 1970-1990's	Diversity fields	Marketing Legal communication and conversation Land reformation Science philosophy Debates methods of anthropology Post-colonial contexts Theory of aesthetics Socialization of military Research operational Social construct to describe origins of race Interpreter of ancient texts Children literacy
			1970's - 2008	As a part of the intellectual lexicon	
	b	In Cyber Age: 1960's - 1990's	1946	Public policy planning	Implemented in Business (scientific management group at Ford Motor Company)

TABLE 5. ***(Continued.)*** **The concepts of social engineering.**

Concept of Social Engineering		Explanation		
Categories	Sub-Categories	Year	Term / Fundamental Ideas	Sub-term
		1948	Cybernetic (tailor-made for ambitious forms of social planning.)	Analogy of Human minds as Turing machines (designing the right game to produce the desired technology).
		1954	Term Scientology (L. Ron Hubbard's)	Cybernetics Enthusiast Science fiction author
		1960's	Cybersecurity	Phone phreaking
		1970's		
			Variant of Social Engineering Attacks	Impersonation Third party authorization Phishing e-mails Utilize pop-up windows Gathering information through dumpster diving
	c) Today		Political Cybersecurity	
Phases of Social Engineering Attacks, that explained by Parthy and Rajendran Research [24]	Information Gathering,		Look at the background of the victim.	View the victim's activity, Lack of moral obligation, Greed, Lack of knowledge about social engineering, Poor cyber attack handling policies.
	Gaining Trust		Build a trust situation.	The victim trusts the hacker, so the victim is willing to give him confidential and important data.
	Exploitation,		Target exploitation.	Hackers began to exploit the target based on the data and information obtained in the previous stage according to the motive of the social engineering attack.
	Exit		Remove traces.	Hackers clean up the traces created during the social engineering stage and leave no clues.
Ethics of social engineering by Hatfield [11]	Virtues Human Hacking		Clarify the critical attributes of the right action so that the ethics of appropriate human behavior can be measured.	Validation of social engineering at the community level, Validation of Penetration Testing activities, Validation of user habits in interacting.
Theories and Principle used concerning social engineering attacks by Yasin et al [15]	Human Factor Priciple		Human intuition is exploited by hackers when interacting with the digital world.	Scarcity, Authority, Liking and similarity, Social proof , Commitment, Reciprocation, Human need and greed, Friendship, Distraction, Curiosity, Deceptive principle, Fear, Dishonesty principle, Trust, Time pressure/urgency, Diffusion of responsibility, Lying, Laziness, Natural inclination to help.
	Related theories		Theories that can be related to social engineering.	Organizational injustice, Technology threat avoidance theory, Routine activity theory, Source credibility theory, Situational crime prevention theory, Theory of planned behavior, Neutralization theory, Learning theory, Protection motivation theory, General deterence theory, Social learning theory, Social bonding theory, General strains theory.

TABLE 5. ***(Continued.)*** **The concepts of social engineering.**

Concept of Social Engineering			Explanation	
Categories	Sub-Categories	Year	Term / Fundamental Ideas	Sub-term
				theory.

9) SOCIAL ENGINEERING PREVENTION STRATEGY

Albladi and Weir, in addition to building a model that is used to identify someone exposed to social engineering attacks, build a semi-automated consulting system that can be used as an approach to grouping social network users according to the type and level of vulnerability of social engineering attacks [16]. The system can advise preventing social engineering attacks on targets due to the grouping mechanism.

Aldawood and Skinner provide recommendations on steps that need to be taken by organizations through interviews with information security and social engineering experts [53]. Interview questions based on the context of awareness of social engineering attacks. Based on the research results, there is a positive relationship between social engineering and user security awareness. Therefore, further research is needed to explore further how increasing awareness of contextually targeted social engineering attacks on organizational culture supports cybersecurity.

Andryukhin provides technical recommendations to prevent social engineering attacks on Blockchain [54]. Recommendations are divided into two based on general social engineering attacks and phishing attacks. Andryukhin did not simulate the technical recommendations given, so it was challenging to develop this research. However, Andryukhin provided research directions in his future, namely a public policy that can protect Blockchain users.

Mouton *et al.* [55] built ten templates that provide detailed steps and phases across social engineering attacks. This attack template covers all communication lines, namely unidirectional, bidirectional and indirect. This template helps map out how social engineering attack schemes can be carried out in the real world. The research of Mouton *et al.* [55] still needs to be developed, especially to build a suitable model to validate social engineering attacks that use each of these communication channels.

Tayouri [56] provides formal policy recommendations about interacting on social media to employees, such as providing cyber security training starting from elementary school or when children are familiar with the internet. Social networks can identify threats from within the organization by analyzing social media content so that the combination of training and education can reduce the risk and impact of social engineering attacks.

10) SOCIAL ENGINEERING DEFENSE FRAMEWORKS

Albladi and Weir build a framework that focuses on humans based on four perspectives: socio-psychological, habitual, socio-emotional, and perceptual [14]. The framework is built based on integrating literature review and relevant theory. The framework has been tested using expert review techniques, especially on the dimensions and attributes used. However, the framework proposed by Albladi and Weir has never been tested in actual cases. The validity of that framework that has been built cannot be measured.

Heartfield and Loukas [12] developed a defense framework against social engineering attacks focusing on humans as sensors to detect and report the existence of social engineering attacks (Human-as-a-Security-Sensor framework). The built framework is very dependent on users reporting social engineering attacks. Unlike the framework built by Albladi and Weir [14], Heartfield and Loukas [12] tested the framework in actual cases. The Human-as-a-Security-Sensor architecture consists of three main processes: detection, classification, and response. The Human-as-a-Security-Sensor framework has drawbacks, primarily when implemented on smartphones and embedded systems. The display of information is not the same between computers and smartphones, and embedded systems, such as not showing the full address of the URL in the browser. That will make it difficult for users to identify social engineering attacks, where users play an essential role in the Human-as-a-Security-Sensor framework.

11) ARTIFICIAL INTELLIGENCE APPROACH

Kumar *et al.* [37] developed a technique for detecting and preventing profile cloning attacks on social networks. Profile cloning is a type of user identity theft to duplicate a stolen profile using valid credentials. The collaboration of machine learning processes and similarity index parameters has succeeded in detecting cloned profiles. Educating users about the dangers of fully displayed profile information will be a challenge in the future. Therefore, an educational model is needed to reduce profile cloning attacks, such as learning about profile settings, validating friendship lines, and not clicking on unknown links on social networks.

A.A.A and P.K [57] developed a phishing attack detection approach that focuses on fast response times and high accuracy. A.A.A and P.K combines URL Blacklist, URL Whitelist, and search engine techniques. Blacklist URLs contain URLs suspected of being phishing links, while Whitelist URLs contain URLs that are considered legitimate URLs. Search engine techniques serve to obtain additional information from URLs, such as domain names, website titles, and query results. The technique proposed by A.A.A and P.K needs to be improved, especially in automatically recognizing Blacklist and Whitelist URLs.

Sandouka *et al.* developed a feature extraction technique that neural networks can use to detect social engineering attacks [58]. Feature identification is carried out on phone

TABLE 6. Social engineering attacks prevention aspects.

			Aspect												
No	Research	Year	Social Engineering Policy	Prevention Protocol	User Studies	Feasibility Social Engineering Attacks	Socio-Technical	Susceptibility Social Engineering Model	Personality and Behavioral Processing	Construct Evaluation	Social Engineering Prevention Strategy	Social Engineering Defense Framework	Artificial Intelligence Approach	Privacy Evaluation	Evaluation Social Engineering Model
1.	[40]		√	-	-	-	-	-	-	-	-	-	-	-	-
2.	[41]		√	-	-	-	-	-	-	-	-	-	-	-	-
3.	[21]		-	√	-	-	-	-	-	-	-	-	-	-	-
4.	[4]		-	-	√	-	-	-	-	√	-	-	-	-	-
5.	[10]		-	-	√	-	-	-	-	-	-	-	-	-	-
6.	[13]		-	-	√	-	-	√	-	-	-	-	-	-	-
7.	[14]		-	-	√	-	-	-	-	√	-	√	-	-	-
8.	[16]		-	-	√	-	-	√	-	√	√	-	-	-	-
9.	[19]		-	-	√	-	-	-	-	√	-	-	-	√	-
10.	[23]		-	-	√	-	-	-	-	-	-	-	-	√	-
11.	[42]		-	-	√	-	-	-	-	-	-	-	-	-	-
12.	[43]		-	-	√	-	-	-	-	-	-	-	-	-	-
13.	[44]		-	-	√	-	-	-	-	-	-	-	-	-	-
14.	[15]		-	-	-	√	-	-	-	-	-	-	-	-	-
15.	[38]		-	-	-	√	-	-	-	-	-	-	-	-	-
16.	[11]		-	-	-	√	-	-	-	-	-	-	-	-	-
17.	[24]		-	-	-	-	√	-	-	-	-	-	-	-	-
18.	[25]		-	-	-	-	√	-	-	-	-	-	-	-	-
19.	[46]		-	-	-	-	√	-	-	-	-	-	-	-	-
20.	[47]		-	-	-	-	√	-	-	-	-	-	-	-	-
21.	[48]		-	-	-	-	√	-	-	-	-	-	-	-	-
22.	[49]		-	-	-	-	-	√	-	-	-	-	-	-	-
23.	[36]		-	-	-	-	-	√	-	-	-	-	-	-	-
24.	[50]		-	-	-	-	-	√	-	-	-	-	-	-	-
25.	[51]		-	-	-	-	-	-	√	-	-	-	-	-	-
26.	[52]		-	-	-	-	-	-	√	√	-	-	-	-	-
27.	[53]		-	-	-	-	-	-	-	-	√	-	-	-	-
28.	[54]		-	-	-	-	-	-	-	-	√	-	-	-	-
29.	[55]		-	-	-	-	-	-	-	-	√	-	-	-	-
30.	[56]		-	-	-	-	-	-	-	-	√	-	-	-	-
31.	[12]		-	-	-	-	-	-	-	-	-	√	-	-	-
32.	[57]		-	-	-	-	-	-	-	-	-	-	√	-	-
33.	[58]		-	-	-	-	-	-	-	-	-	-	√	-	-
34.	[59]		-	-	-	-	-	-	-	-	-	-	√	-	-
35.	[60]		-	-	-	-	-	-	-	-	-	-	√	-	-
36.	[61]		-	-	-	-	-	-	-	-	-	-	√	-	-
37.	[62]		-	-	-	-	-	-	-	-	-	-	√	-	-
38.	[37]		-	-	-	-	-	-	-	-	-	-	√	-	-
39.	[26]		-	-	-	-	-	-	-	-	-	-	-	√	-
40.	[20]		-	-	-	-	-	-	-	-	-	-	-	√	-
41.	[63]		-	-	-	-	-	-	-	-	-	-	-	-	√
42.	[64]		-	-	-	-	-	-	-	-	-	-	-	-	√
43.	[65]		-	-	-	-	-	-	-	-	-	-	-	-	√
44.	[66]		-	-	-	-	-	-	-	-	-	-	-	-	√
45.	[67]		-	-	-	-	-	-	-	-	-	-	-	-	√
46.	[68]		-	-	-	-	-	-	-	-	-	-	-	-	√

calls or callers to determine whether these features include social engineering attacks or not. The features that have been identified are voice identification, request for confidential information, request for passwords, install programs. This feature is obtained based on a dataset of conversations that have been identified as social engineering attacks. The resulting features are minimal and not tested in actual conditions. Therefore, to develop this research, it is necessary to identify additional features, such as call time, call frequency, and call duration.

Heartfield *et al.* use machine learning to ensure the reliability of social engineering attack reports provided by users [59]. Reports of social engineering attacks are generated from a controlled experiment, in which users perform activities such

TABLE 7. Social engineering attacks prevention approaches.

No	Research	Aproaches				
		Protocol	Method	Framework	Model	Evaluation
1	[10]	-	Health campaigns	-	-	-
2	[21]	Co-utile	Simulation		Formal	
3	[16]	-	Questionaire		User vulnerability	-
4	[15]		Interview		Social Engineering Attack Game based Analysis	Empirical
5	[63]		Finite State Machine		Mitigation and Prevention Social Engineering Phising Based on Facebook	Validating based on realistic scenario
6	[69]		Machine learning		Phising Detection based on Machine Learning	Performance
7	[54]		Combine technical and social prevention techniques			-
8	[37]		Machine learning and recomendation			-
9	[70]		Machine learning			Performance
10	[34]		Interview and Questionaire			-
11	[57]		Blacklist method or whitelist method or search engine based technique			Accuracy and time consuming
12	[42]		Semi-structured interviews			-
13	[50]		Questionaire		Enhanced Domain-Specific Risk-Taking scale (DOSPERT) and General Decision-Making Style scale (GDMS)	Factor analysis, reliability testing, multicollinearity, variance, multiple exact logistic regression
14	[71]		Controlled experiment		-	-
15	[12]		-	Human-as-a-security-sensor framework		Expert review and performance
16	[14]			User Centric		Expert review, realibility, One sample t-test.
17	[72]			Detection of Online Manipulation		-

as reading email, social media, and browsing. Controlled experiments such as those carried out by Heartfield *et al.* have weaknesses, such as users participating in this research being wary because social engineering attacks will test them.

Lansley *et al.* use Natural Language Processing (NLP) and Artificial Neural Network (ANN) techniques to detect social engineering attacks [60]. NLP technique is used to decipher the text of the conversation and then look for grammatical errors, while ANN is used to classify the results of the NLP process, whether it is a social engineering attack or not. The collaboration of NLP and ANN techniques produces high accuracy, but it has never been tested on a balanced dataset, with more attributes and actual conditions.

Masoud *et al.* used the Back Propagation Neural Network (BPNN) technique to prevent website phishing attacks with a Software Define Network (SDN) approach [61]. When users access phishing websites, the concept of Masoud *et al.* managed to restore a legitimate website from the phishing website.

Zambrano *et al.* use machine learning techniques to detect social engineering attacks that apply in some instances, such as grooming [62]. Grooming is a procedural criminal activity used by pedophiles to arrest their victims using internet access. Zambrano *et al.* used a dataset containing Grooming conversations, then extracted these conversations using NLP techniques. After that, the classification process determines whether the conversation has a grooming attack. The limitations of the technical capabilities tested on the dataset require that Zambrano *et al.* added some recommendations for research development such as general conversation data and sexuality as a comparison of grooming conversations.

12) PRIVACY EVALUATION

Other methods would view from four research studies. Analyzed Sybil attack on the social network used three steps—built graph on social network case, separated interactions characteristic both of user and their community, then used DFS algorithms to determine essential characteristics of Sybil attacks [26]. In this research, a process takes place that quantifies the privacy of social networks while empirical and theoretical methods were made on the active attack. The theoretical section explained the basic notation of formalized optimization problems [20]. The theoretical section's result is a metric anti-dimensional graph with a solution algorithm for attackers manipulating alpha nodes and a revised estimation algorithm. This overall research result is a network manager who made the cycle network topology and privacy problem over eight social networks. This result was done by appraising sixteen factors to determine social networks' security and privacy [19]. These sixteen factors, such as user setup privacy, communication about information and social network content, security setup of social network account, and information sharing. Analysis of the anonymization algorithm used to have a high impact on graph utility [23]. Research on privacy evaluation still needs development in several aspects, such as implementation in different cases [26], [20], data complexity and data usability [23], and collaboration with several related theories [19].

13) EVALUATION SOCIAL ENGINEERING MODEL

Jamil *et al.* developed a model that aims to detect and prevent social engineering attacks, especially phishing attacks on Facebook [63]. The built model was tested in real terms with four scenarios in a Finite State Machine. Model testing is done with JFLAP tools, a tool used to test and track formal language concepts and automata theory. However, Jamil's research could not detect social engineering attacks that rely on URL spoofing.

Mouton *et al.* built a model to evaluate social engineering attacks [64]. This model uses a decision tree and breaks down the process into more manageable components to assist decision-making. This model is the development of Mouton *et al.* [65], with the addition of dealing with three categories of social engineering attacks. Mouton *et al.* [65] consist only of direct two-way communication between the attacker and the victim. The model developed by Mouton *et al.* [64] was tested using common social engineering attacks. The model developed by Mouton *et al.* [64] provides a standard procedural template for detecting social engineering attacks, so Mouton *et al.* [66], [67] used the Finite State Machine (FSM) to provide further a more abstract and extensible model based on the interconnections between different tasks and scenarios. FSM can facilitate the incorporation of specific extensions in an organization by grouping similar activities into different categories and subdividing them into one or more circumstances. The FSM-based social engineering model [66], [67] was tested on three communication streams, namely unidirectional, two-way and indirect. Research conducted by Mouton *et al.* [66], [67] cannot stand alone when implemented in organizations. It requires awareness and reasonable information security policies.

Wang *et al.* [68] built a social engineering ontology domain in the cybersecurity field, then evaluated the domain. It also builds a knowledge graph based on 15 incidents and social engineering attack scenarios. Collaboration between ontology and knowledge graphs can find potential attackers, targets and attack paths, and social engineering threat elements such as human vulnerabilities and attack media. Research Wang *et al.* [68] needs to be validated in actual cases to strengthen the study results further.

The summary of the social engineering attacks prevention aspect can be viewed in Table 6.

V. CONCLUSION AND FUTURE WORK

Previous research has established methods and frameworks for social engineering attacks prevention; moreover, social engineering attacks are still unpredictable for unsuspected victims. Different cases and actors, especially for social media or social network cases, can modify social engineering attack techniques.

Based on this systematic literature review, a research was found on prevention protocol to set up information sharing over a social network, seven research on user studies, three research about social engineering attacks prevention concepts, two research on others concepts, a research on the social engineering attacks prevention model, six research about framework construct, a research of framework dimension, two research of social engineering attacks prevention framework, a research about social engineering attacks prevention method, four research of other methods, and six research about framework evaluation.

There are three main research areas in the approach of social engineering attacks prevention—health campaigns to resist social engineering attacks, user vulnerability of social engineering victims, and co-utile protocol to protect information disclosure on social media. Best ways of health campaigns depend on the scope of audience and content of that's campaigns. The campaign for both of adults and teenagers also had difference tactics. The goodness content of campaign also affected to decrease the hazard of social engineering attacks. The model of user vulnerability for social engineering victims could took some recommendation of social engineering knowledge in social network. This model also, was used to tested user vulnerability based on risk assessment of user response. The testing of this model was used to revoke privacy boundaries or to shared confidential and private information in social network. Co-utile protocol could make the exchange of information among users of social media and included user reputation to decrease the diffidence of users from sharing private information with other people.

Based on our review, several works can support the social engineering attacks prevention. The reviews we found can be used by practitioners and information security experts in overcoming social engineering attacks. They can carry out development based on a collaboration of several approaches such as protocols, methods, frameworks, models and evaluations to prevent social engineering attacks.

ACKNOWLEDGMENT

This work was supported in part by the Malaysia Ministry of Education, Universiti Kebangsaan Malaysia, under Grant KKP/2020/UKM/4/3.

REFERENCES

[1] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Comput. Secur.*, vol. 73, pp. 102–113, Mar. 2018.

[2] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment recommendations of the National Institute of Standards and Technology (SP 800-115)," NIST Special Publication, 2008, pp. 1–80, vol. 800. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-115/final

[3] M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Comput. Hum. Behav.*, vol. 66, pp. 75–87, Jan. 2017.

[4] R. Syed, "Enterprise reputation threats on social media: A case of data breach framing," *J. Strategic Inf. Syst.*, vol. 28, no. 3, pp. 257–274, Sep. 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0963868718300064

[5] Verizon, A. J. Nathan, and A. Scobell. (2020). *2020 Data Breach Investigations Report*. [Online]. Available: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[6] A. H. Shaari, M. R. Kamaluddin, W. F. P. Fauzi, and M. Mohd, "Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims," *GEMA Online J. Lang. Stud.*, vol. 19, no. 1, pp. 97–115, 2019, doi: 10.17576/gema-2019-1901-06.

[7] M. R. A. Rahman, "Online scammers and their mules in Malaysia," *Jurnal Undang-Undang dan Masyarakat*, vol. 26, no. 2020, pp. 65–72, 2020, doi: 10.17576/juum-2020-26-08.

[8] T. S. Ming, N. L. Shi, and A. M. Taha, "Awareness of the risks and dangers of social networking: Exploration on four types of Malaysian secondary schools," *J. Komunikasi, Malaysian J. Commun.*, vol. 36, no. 1, pp. 147–165, 2020, doi: 10.17576/JKMJC-2020-3601-09.

[9] A. Jamil, M. S. Hassan, N. M. Salleh, and R. Yaakob, "Non-financial risk disclosure: From narratives to an index based on Delphi technique," *Asian J. Government*, vol. 14, pp. 1–19, 2020, doi: 10.17576/ajag-2020-14-10.

[10] N. Abe and M. Soltys, "Deploying health campaign strategies to defend against social engineering threats," *Procedia Comput. Sci.*, vol. 159, pp. 824–831, 2019.

[11] J. M. Hatfield, "Virtuous human hacking: The ethics of social engineering in penetration-testing," *Comput. Secur.*, vol. 83, pp. 354–366, Jun. 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S016740481831174X

[12] R. Heartfield and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework," *Comput. Secur.*, vol. 76, pp. 101–127, Jul. 2018.

[13] E. D. Frauenstein and S. Flowerday, "Susceptibility to phishing on social network sites: A personality information processing model," *Comput. Secur.*, vol. 94, p. 101862, Jul. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404820301346

[14] S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Hum.-Centric Comput. Inf. Sci.*, vol. 8, no. 1, p. 5, Dec. 2018.

[15] A. Yasin, R. Fatima, L. Liu, A. Yasin, and J. Wang, "Contemplating social engineering studies and attack scenarios: A review study," *Secur. Privacy*, vol. 2, no. 4, pp. 1–14, Jul. 2019.

[16] S. M. Albladi and G. R. S. Weir, "Predicting individuals' vulnerability to social engineering in social networks," *Cybersecurity*, vol. 3, no. 1, 2020.

[17] Y. M. Yusof and D. Singh, "Civil servants awareness guideline towards computer security policy: A case study at the manpower department, ministry of human resources," *Asia–Pacific J. Inf. Technol. Multimedia*, vol. 10, no. 8, pp. 86–99, 2021, doi: 10.17576/apjitm-2021-1001-08.

[18] M. A. Pitchan, S. Z. Omar, and A. H. A. Ghazali, "Amalan keselamatan siber pengguna internet terhadap buli siber, pornografi, E-mel phishing dan pembelian dalam talian," *Jurnal Komunikasi, Malaysian J. Commun.*, vol. 35, no. 3, pp. 212–227, 2019.

[19] P. van Schaik, J. Jansen, J. Onibokun, J. Camp, and P. Kusev, "Security and privacy in online social networking: Risk perceptions and precautionary behaviour," *Comput. Hum. Behav.*, vol. 78, pp. 283–297, 2018.

[20] B. DasGupta, N. Mobasheri, and I. G. Yero, "On analyzing and evaluating privacy measures for social networks under active attack," *Inf. Sci.*, vol. 473, pp. 87–100, 2019.

[21] D. Sánchez, J. Domingo-Ferrer, and S. Martínez, "Co-utile disclosure of private data in social networks," *Inf. Sci.*, vol. 441, pp. 50–65, 2018.

[22] Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: Overview and new direction," *Future Gener. Comput. Syst.*, vol. 86, pp. 914–925, 2018.

[23] C. Zhang, H. Jiang, X. Cheng, F. Zhao, Z. Cai, and Z. Tian, "Utility analysis on privacy-preservation algorithms for online social networks: An empirical study," *Pers. Ubiquitous Comput.*, vol. 25, no. 6, pp. 1063-1079, 2021.

[24] R. A. M. Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1, p. 10, Dec. 2020.

[25] S. P. Velayudhan and M. S. B. Somasundaram, "Compromised account detection in online social networks: A survey," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 20, pp. 1–15, Oct. 2019.

[26] H. Asadian and H. H. S. Javadi, "Identification of Sybil attacks on social networks using a framework based on user interactions," *Secur. Privacy*, vol. 1, no. 2, p. e19, Mar. 2018.

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

[28] J. W. Bullee and M. Junger, "How effective are social engineering interventions? A meta-analysis," *Inf. Comput. Secur.*, vol. 28, no. 5, pp. 801–830, 2020.

[29] P. Schaab, K. Beckers, and S. Pape, "Social engineering defence mechanisms and counteracting training strategies," *Inf. Comput. Secur.*, vol. 25, no. 2, pp. 206–222, Jun. 2017.

[30] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, 2019.

[31] Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, 2020.

[32] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021.

[33] A. Bryman and E. Bell, *Business Research Methods*, 3rd ed. New York, NY, USA: Oxford Univ. Press, 2011.

[34] V. Gomes, J. Reis, and B. Alturas, "Social engineering and the dangers of phishing," in *Proc. Iberian Conf. Inf. Syst. Technol.*, Jun. 2020, pp. 24–27. [Online]. Available: https://ieeexplore.ieee.org/document/9140445/

[35] P. Zambrano, J. Torres, and P. Flores, "How does grooming fit into social engineering?" in *Advances in Intelligent Systems and Computing*, vol. 924. Singapore: Springer, 2019, pp. 629–639.

[36] A. Algarni, Y. Xu, and T. Chan, "An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 661–687, Nov. 2017. [Online]. Available: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1559&context=icis2015

[37] N. Kumar, P. Dabas, and Komal, "Detection and prevention of profile cloning in online social networks," in *Proc. 5th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Oct. 2019, pp. 287–291. [Online]. Available: https://ieeexplore.ieee.org/document/8988394/

[38] P. P. Parthy and G. Rajendran, "Identification and prevention of social engineering attacks on an enterprise," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8888441/

[39] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, "SoK: A comprehensive reexamination of phishing research from the security perspective," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 671–708, 2020.

[40] N. Z. Khidzir, S. A. Ahmed, and T. T. Guan, "Management policies for the prevention technique of social engineering (SoE) attacks in the organization," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 10, pp. 78–82, 2019.

[41] H. A. Aldawood and G. Skinner, "A critical appraisal of contemporary cyber security social engineering solutions: Measures, policies, tools and applications," in *Proc. 26th Int. Conf. Syst. Eng. (ICSEng)*, Dec. 2018, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8638166/

[42] P. Burda, L. Allodi, and N. Zannone, "Don't forget the human: A crowdsourced approach to automate response and containment against spear phishing attacks," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 471–476. [Online]. Available: https://ieeexplore.ieee.org/document/9229829/

[43] R. Bleiman and A. Rege, "An examination in social engineering: The susceptibility of disclosing private security information in college students," in *Proc. 15th Int. Conf. Cyber Warfare Secur. (ICCWS)*, 2020, pp. 47–56.

[44] P. M. W. Musuva, C. Chepken, and K. Getao, "A naturalistic methodology for assessing susceptibility to social engineering through phishing," *Afr. J. Inf. Syst.*, vol. 11, no. 3, pp. 157–182, 2019. [Online]. Available: https://digitalcommons.kennesaw.edu/ajis/vol11/iss3/2

[45] P. P. Parthy and G. Rajendran, "Identification and prevention of social engineering attacks on an enterprise," pp. 2–6, 2016.

[46] A. Ferreira, "Why ransomware needs a human touch," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2018, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8585650/

[47] R. Heartfield, G. Loukas, and D. Gan, "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks," *IEEE Access*, vol. 4, pp. 6910–6928, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7587431/

[48] B. Banire, D. Al Thani, and Y. Yang, "Investigating the experience of social engineering victims: Exploratory and user testing study," *Electronics*, vol. 10, no. 21, 2021.

[49] A. Alturki, N. Alshwihi, and A. Algarni, "Factors influencing players' susceptibility to social engineering in social gaming networks," *IEEE Access*, vol. 8, pp. 97383–97391, 2020.

[50] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process," *IEEE Access*, vol. 9, pp. 44928–44949, 2021.

[51] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, p. 1, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7576667/

[52] F. Amato *et al.*, "Recognizing human behaviours in online social networks," *Comput. Secur.*, vol. 74, pp. 355–370, May 2018.

[53] H. Aldawood and G. Skinner, "Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions," *IEEE Access*, vol. 8, pp. 67321–67329, 2020.

[54] A. A. Andryukhin, "Phishing attacks and preventions in blockchain based projects," in *Proc. Int. Conf. Eng. Technol. Comput. Sci. (EnT)*, Mar. 2019, pp. 15–19. [Online]. Available: https://ieeexplore.ieee.org/document/8711898/

[55] F. Mouton, L. Leenen, and H. S. S. Venter, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, vol. 59, pp. 186–209, Jun. 2016.

[56] D. Tayouri, "The human factor in the social media security—Combining education and technology to reduce social engineering risks and damages," *Procedia Manuf.*, vol. 3, no. Ahfe, pp. 1096–1100, 2015.

[57] A. A. Athulya and K. Praveen, "Towards the detection of phishing attacks," in *Proc. 4th Int. Conf. Trends Electron. Inform. (ICOEI)*, Jun. 2020, pp. 337–343.

[58] H. Sandouka, A. J. Cullen, and I. Mann, "Social engineering detection using neural networks," in *Proc. Int. Conf. CyberWorlds*, 2009, pp. 273–278. [Online]. Available: http://ieeexplore.ieee.org/document/5279574/

[59] R. Heartfield, G. Loukas, and D. Gan, "An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks," in *Proc. 15th IEEE/ACIS Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA)*, Jun. 2017, pp. 371–378. [Online]. Available: http://ieeexplore.ieee.org/document/7965754/

[60] M. Lansley, F. Mouton, S. Kapetanakis, and N. Polatidis, "SEADEr++: Social engineering attack detection in online environments using machine learning," *J. Inf. Telecommun.*, vol. 4, no. 3, pp. 346–362, 2020.

[61] M. Masoud, Y. Jaradat, and A. Q. Ahmad, "On tackling social engineering web phishing attacks utilizing software defined networks (SDN) approach," in *Proc. 2nd Int. Conf. Open Source Softw. Comput. (OSSCOM)*, Dec. 2016, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7863679/

[62] P. Zambrano *et al.*, "Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach," *IEEE Access*, vol. 7, pp. 142129–142146, 2019.

[63] A. Jamil, K. Asif, Z. Ghulam, M. K. Nazir, S. M. Alam, and R. Ashraf, "MPMPA: A mitigation and prevention model for social engineering based phishing attacks on Facebook," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 5040–5048. [Online]. Available: https://ieeexplore.ieee.org/document/8622505/

[64] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack detection model: SEADMv2," in *Proc. Int. Conf. Cyberworlds (CW)*, Oct. 2015, pp. 216–223. [Online]. Available: https://ieeexplore.ieee.org/document/7398418

[65] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an ontological model defining the social engineering domain," in *ICT and Society* (IFIP Advances in Information and Communication Technology), vol. 431. Sep. 2015, pp. 266–279.

[66] F. Mouton, A. Nottingham, L. Leenen, and H. Venter, "Finite state machine for the social engineering attack detection model: SEADM," *SAIEE Africa Res. J.*, vol. 109, no. 2, pp. 133–148, Jun. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8531953/

[67] F. Mouton, A. Nottingham, L. Leenen, and H. S. S. Venter, "Underlying finite state machine for the social engineering attack detection model," in *Proc. Inf. Secur. South Africa*, Jun. 2017, vol. 109, no. 2, pp. 98–105. [Online]. Available: http://ieeexplore.ieee.org/document/8251781/

[68] Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social engineering in cybersecurity: A domain ontology and knowledge graph application examples," *Cybersecurity*, vol. 4, no. 1, 2021.

[69] M. Rastogi, A. Chhetri, D. K. Singh, and G. Rajan V, "Survey on detection and prevention of phishing websites using machine learning," in *Proc. Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, vol. 7, Mar. 2021, pp. 78–82. [Online]. Available: https://ieeexplore.ieee.org/document/9404714/

[70] C. Singh and Meenu, "Phishing website detection based on machine learning: A survey," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2020, pp. 398–404. [Online]. Available: https://ieeexplore.ieee.org/document/9074400/

[71] M. Adil, R. Khan, and M. A. N. Ul Ghani, "Preventive techniques of phishing attacks in networks," in *Proc. 3rd Int. Conf. Advancements Comput. Sci. (ICACS)*, Feb. 2020, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/document/9055943/

[72] S. Java, F. L. Basheer, S. Riaz, M. J. Kaur, and A. Mushtaq, "Detection of online manipulation to prevent users victimization," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 593–599. [Online]. Available: https://ieeexplore.ieee.org/document/8701330/

WENNI SYAFITRI is currently pursuing the Ph.D. degree with the Center for Cyber Security, Universiti Kebangsaan Malaysia, Malaysia. Her work has been published in Journal IOP, Core IT, Digital Zone, and Dinamisia. Her research interests include information security, risk management, knowledge management, software engineering, and IS/IT strategic planning.

ZARINA SHUKUR received the Ph.D. degree from the University of Nottingham, in 1999. She is currently a Professor at the Cyber Security Center, Universiti Kebangsaan Malaysia. Her work has been published in *International Journal of Advanced Computer Science and Applications*, *Information and Software Technology*, and *Journal of Computer Science*. Her research interests include formal methods and cybersecurity.

UMI ASMA' MOKHTAR is currently a Senior Lecturer of information science at the School of Information Technology, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. She is also a Co-Researcher of InterPARES Trust Project for Malaysian Team. Her papers have been published in international and national journals, including the *International Journal of Information Management* and *Records Management Journal*. Her research interests include electronic records management, function-based classification, and information policy. She was a recipient of the Oliver Wendell Holmes Travel Award from the Society of American Archivists, in 2012.

ROSSILAWATI SULAIMAN received the B.Sc. degree in computer science from Universiti Kebangsaan Malaysia, in 2000, the M.Sc. degree in computer science from the University of Essex, U.K., in 2003, and the Ph.D. degree from the University of Canberra, in 2011. She is currently a Senior Lecturer at Universiti Kebangsaan Malaysia. Her work has been published in *Journal Theoretical and Applied Information Technology*, *International Journal of Advanced Computer Science and Applications*, and *Journal of Computer Science*. Her research interests include steganography and applied cryptography.

MUHAMMAD AZWAN IBRAHIM received the bachelor's degree in electrical engineering from Universiti Teknologi Mara, Malaysia, and the M.E. and Ph.D. degrees in communication and computer from Universiti Kebangsaan Malaysia. He is currently a Senior Metrologist at the Electrical Group, National Metrology Institute of Malaysia.