Methodological Review of Social Engineering Policy Model for Digital Marketing

Wenni Syafitri, Zarina Shukur, Umi Asma' Mokhtar, Rossilawati Sulaiman
Center for Cyber Security-Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, Bangi Selangor, Malaysia

***Abstract*—Social engineering attacks are recognized as human-based threats and continue to increase, despite studies focusing on prevention methods that do not rely on the human aspect. The impacts of these attacks are felt across various industries and organizations. To solve this issue, a social engineering policy model must be proposed for prevention in industrial settings, particularly emphasizing digital marketing activities, a crucial process in contemporary industries. However, hackers often exploit activities or information in these practices, necessitating an industry-specific policy to prevent these threats in digital marketing. As a result, a comprehensive review was conducted to identify critical method for develop social engineering policy model. The review uses Bryman's method to determine effective approaches for designing a social engineering policy model tailored for digital marketing. Consequently, this review provided a method for crafting effective social engineering policy, providing valuable insights for enhancing digital marketing security.**

***Keywords*—Digital marketing; social engineering attack prevention; review study; security policy model**

I. INTRODUCTION

Social engineering attacks are often performed to expose private information through unauthorized actions [1]. Similarly, NIST describes social engineering attacks as a method of getting trust and confidence from victims [2]. Verizon defines social engineering as exploring human psychology and manipulating sensitive information to exploit people's vulnerability [3].

Various methods have been used to prevent social engineering attacks. For example, CISA recommends practices such as staying vigilant, verifying phone calls and emails, refraining from divulging private or organizational information, ensuring email safety for financial transactions, installing, and managing antivirus software, implementing email filtering and firewall protection, using anti-phishing features in emails and browser plugins, and using multi-factor authentication (CISA). SANS Institute also advocates for security awareness training to mitigate the impact of social engineering attacks (SANS). Moreover, it is crucial to be aware that the prevention methods proposed by CISA and SANS primarily address the technical aspects.

The term "social engineering" is applicable in the context of information security and marketing. Typically, marketing practices can be viewed as a form of social engineering [4]. In marketing, social engineering comprises applied methods for influencing social impact or change, signifying practices used to influence people's decisions [5]. Consequently, activities in marketing can be termed social engineering [6].

The growing trend of organizations engaging in digital marketing to communicate with external parties makes organizational boundaries unclear. This complicates decisions regarding the information that can be shared with external partners [7]. For example, using social media for digital marketing, including advertising, introduces the risk of unintended information leakage.

According to the Weekly Threat Report dated April 12, 2021, published by NSCS, a data breach compromised 553 million social network users in 106 countries. This breach exposed private information such as IDs, gender, location, and date of birth (NSCS). Unauthorized individuals may exploit this information, manipulating human weaknesses to acquire more confidential data for financial gain. This deceptive tactic is executed through social engineering attack methods. The study conducted by [8] and [9] defined marketing studies based on the respective methods and scopes regarding social engineering. Unlimited exploitation of privacy can cause problems for both customers and companies, leading to a loss of customer trust and revenue when not properly managed by the company.

Cybersecurity policy has a significant influence in fostering cyber governance and cyber resilience in organizations [10], [11]. Some researchers try to build cybersecurity policies with several techniques, such as identifying appropriate security policies to be applied to cyberspace [12], identifying awareness of cybersecurity policies [13], and conducting comparisons between two countries in terms of governance aspects and security policies [14]. However, the policies are to be built by [12], [13], and [14] generalized against various attacks so that prevention against social attacks cannot be used. Therefore, [10] suggested that building policies against cyber-attacks should be specific, such as policies to prevent social engineering attacks.

Very few studies have built social engineering policies. The study in [15] examined recommendations for dealing with organizational members who fall prey to social engineering as an organizational policy issue. The results of this analysis showed that participants did not favor a punitive approach to security failures. Instead, they tended to favor education as a more pragmatic and humane solution. In contrast to [10], they combine the principles of raising security awareness and education in building a social engineering policy. The concept proposed by [10] requires organizational members to read and

learn how social engineering attacks work. In addition, social engineering attack awareness training is required to support the learning activities of organizational members, such as bringing in experts if they have the budget [16].

The studies in [15] and [10] specifically do not focus on building social engineering attack policies. They focus more on policies toward victims of social engineering attacks [15] and policies on how to enhance the social engineering knowledge of each member of the organization [10]. None of the researchers discussed how to build a social engineering policy. Therefore, to answer the gap that researchers have not resolved, this study propose a technical way to design a social engineering policy with a focus on digital marketing. The specialized policy aims to identify and implement relevant policy rules [10].

Developing and consistently updating information security policy is essential for enhancing an organization's security culture [17]. Numerous studies recommend adapting social engineering attack prevention methods at the organizational level by implementing robust social engineering attack policy. The study in [18] proposed the establishment of a strong information security culture through a policy aimed at preventing social engineering attacks. This implies that the crafted information security policy needs to anticipate recent trends in social engineering attacks [19]. Additionally, [15] advised focusing on content rather than just attack policy, taking into account factors such as avoiding harsh sanctions, providing employee education, offering incentives for positive behavior, and determining the appropriate timing for administering punishments.

A good organization should develop and evaluate security policy based on relevant standards and business processes to manage systems, applications, and information effectively. Implementation of social engineering policy by organizations can mitigate vulnerability to hacker attacks, thereby minimizing potential damage [20]. NIST SP 800-152 establishes a standard for Cryptographic Key Management Systems (CKMS), which categorizes security policy into two levels, namely a high-level policy for managing organizational information and a low-level policy consisting of rules to safeguard this information (NIST). CKMS standard is structured with three layers of security policy, including action management, information security, and cryptographic key management system security policy. NIST SP 800-53 Revision 4 defines security policy as a set of standards that support security services.

The search activity showed 31 studies on security policy, each categorized based on the security policy aspects. Each study used a unique method with the primary goal of developing a security policy, aiming to identify an appropriate phase for designing a security policy model to prevent social engineering attacks, particularly in digital marketing.

In the subsequent sections of this paper, studies on the security policy are explained in Section II. Meanwhile, Section III outlines the methodology, Section IV presents the results, Section V presents discussion and Section VI contains the conclusion.

II. Related Work

This section explains some closely related studies, focusing on the topics, challenges, and recommendations relevant to the objective of this current study. The mentioned articles serve as references for designing a security policy model to prevent social engineering attacks in digital marketing. Consequently, the related studies are categorized into four sections as follows:

A. Social Engineering in Digital Marketing

Social engineering has a unique significance in digital marketing, where various marketing activities, such as content marketing, inbound marketing, influencer marketing, social media marketing, creative marketing, innovation marketing, customer journey marketing, conversational marketing, customized lifecycle marketing, performance marketing, and Marketing 4.0 & 5.0, are categorized as forms of social engineering [6].

Social marketing is loosely associated with various marketing methods (as shown in Table I), including non-profit marketing, charity marketing, cause-related marketing, public sector marketing, and government marketing. Additionally, it shares ties with more commercial activities including green marketing or branding for charitable causes, where a company aims to be recognized as a socially responsible entity [8]. When social marketing is used by governments, it does not carry the same negative connotation as totalitarian regimes' propaganda, even though it is a routine government activity [8]. Social engineering is often linked to the desired outcomes of a totalitarian state and is commonly associated with the oppression of citizens in the public perception [8]. Consequently, social engineering is typically viewed as unfavorable, while social marketing is seen as positive.

Digital marketing plays a crucial role in augmenting company income. However, improper use of digital marketing concerning information security can lead to substantial losses for the organization. [8] developed a conceptual model that described the factors related to social engineering and marketing. This model shows the effective and ineffective implementation of social engineering in government activities, such as education, policing, and funding. Similarly, [9] concluded that prioritizing privacy was a viable strategy for increasing hotel revenue. Hotels strategically use privacy measures to provide customers with appropriate services, such as spa and self-service amenities (mini-bars, vending machines, etc.), to enhance perceptions of room comfort and promote repeat visits.

Specific policies are required to address social engineering attacks in organizations, primarily in the aspect of digital marketing. These policies not only help protect sensitive data but also improve the overall effectiveness of marketing campaigns by fostering trust and security among consumers.

In addition, this policy will increase information security awareness as individuals can recognize the nature of cyber threats, how attacks are delivered, their impact on individual safety and business operations, recognize what behaviors can put organizations at risk, and what actions they need to implement when they are attacked [10].

TABLE I. RELATION BETWEEN SOCIAL ENGINEERING AND DIGITAL MARKETING COMPARISON OF A REVIEW STUDY

Term in digital marketing	Digital marketing activity	Related to social engineering activity
Personalization [21]	Marketers utilize browsing history, transaction history, and demographic information to build personalized ads that aim to increase competitive advantage.	Attackers make personalized message content contextually relevant to targets based on collected information [22].
Social Proof [23]	This technique utilizes feedback or ratings from other customers to influence customer decisions in purchasing a product or service.	Attackers create a false sense of security and collective behavior based on fake testimonials or statistics to increase credibility. In addition, the attacker may impersonate a trusted or respected figure in an organization and then say that his or her requests are in line with what everyone else is doing [24].
Scarcity and Urgency [25]	Marketers use the technique of conveying information on commodity unavailability or limited offer of a product in marketing activities.	Attackers using the scarcity principle refer to a persuasion approach using time-based constraints. This technique triggers feelings of anxiety about what will happen if no immediate action is taken.[26].
Storytelling [27]	Marketers create stories around products to create an emotional connection with consumers.	The attacker constructs a personalized story to get the attention of the target, such as a sad story or a victim of a crime or war [28].

Trust is paramount in digital marketing. A well-designed security policy will give customers the impression that the organization takes protecting customers from cybersecurity attacks seriously. The policy must contain an interactional approach to influencing user decisions through recommendations or responses from others as a preventive measure for social engineering attacks [29].

In addition, the social engineering attack policy that has been built is essential to be implemented in an organization. Regular training to raise awareness is an important aspect when implementing social engineering attack policies. Every organization must build social engineering policies carefully to reduce individuals becoming victims of social engineering attacks [15].

The social engineering attack policy should contain technical measures including incident management [30]. Every incident caused by social engineering must be immediately responded to by the organization, either automatically or manually, so as not to have a fatal impact on the management and finances of the organization [31]. Therefore, social engineering attack policies must contain incident management measures that are always up-to-date with social engineering attack patterns [32].

Therefore, building a social engineering attack policy is not only a preventive measure, but digital marketing aspects are an inseparable part of fostering customer trust, ensuring compliance, and protecting the organization from evolving threats.

Very few researchers have modeled social engineering threats such as [33], [34], and [35]. One of the most famous social engineering attacks is phishing [34]. Threat modeling [33] is to build a phishing model consisting of the factors of threat detection, elaboration, phishing susceptibility, motivation to process, ability to process, and knowledge. Threat detection factors have a significant influence on reducing phishing attacks. Organizations should invest in mitigation measures that support users in detecting phishing threats [36]. In addition, the use of phishing threat modeling also has a significant impact on identifying and securing IoT device vulnerabilities during the initial design phase [34]. Reference [34] utilize detailed information about attacks from each stakeholder. After that, Authors in [34] built a Data Flow Diagram (DFD) to apply threat modeling techniques to identify potential threats in the underlying case using STRIDE threat modeling.

In contrast to [35], they predicted the occurrence of social engineering attacks based on data on the effectiveness of the modalities and principles of persuasion used in Social Engineering Threats (SETs). However, the prevention was carried out by [33], [34], and [35]. It is not fully maximized because it still focuses on technical prevention and evaluation of vulnerabilities that have the opportunity to be breached by social engineering.

Some researchers built threat modeling on social networks, such as Privacy Threat Modeling Language (PTMOL) [37] and DetThr model [38]. The study in [37] built PTMOL to model privacy threats in the Online Social Network (OSN) domain. PTMOL can be incorporated into software development during the design phase of OSNs [37] so that software developers can focus more on privacy protection when building OSNs. The DetThr model built by [38] uses the ThrNet semantic network. The study in [38] claimed that the DetThr Model performed very well in identifying threatening tweet messages. Similar to [33], [34], and [35], [38] and [37] have not been able to build a maximum prevention for social engineering attacks because they still focus on privacy and tweet threats technically.

Brand honesty, consumer trust, and economic security are all severely compromised by sophisticated cyberattacks targeting brand communication networks in today's digitally driven market [39].

Social engineering threats are increasingly dangerous today, but very few focus on prevention, especially in digital marketing. Some social engineering attacks that can be used by attackers in digital marketing are phishing, spear phishing, baiting, pretexting, vishing, smishing, and water-Holing [40]. Phishing utilizes human weaknesses such as time constraints, threats, and user habits to obtain important information by using emails that already contain malicious links. Similar to phishing, spearphishing is more targeted to potential victims; likewise, with vishing, phishing techniques utilize phone calls or the like to get victims, while smishing utilizes Short Message Service (SMS). Baiting utilizes the curiosity of potential victims, such as using a USB Stick with a specific

company logo that contains malicious code. At the same time, water-holing takes advantage of the weakness of an organization's website to insert malicious code to obtain important information when the victim accesses the website. Social engineering attacks can utilize digital marketing activities, as shown in Table II.

TABLE II. SOCIAL ENGINEERING WITH ATTACK VECTOR IN DIGITAL MARKETING

Social engineering attack	Attack vector	Potential digital marketing activity to exploit
Phishing	Email or message feature from Social Networking Sites contains a malicious link with a broader target	Email marketing, ads on social media, promotional landing pages, promotion-based instant messaging, Malicious SEO (Search Engine Optimization), Promotion in Online Groups or Forums, and QR Codes in Offline-Online Campaigns.
Spear Phishing	Email or message feature from Social Networking Sites contains a malicious link with a broader target	Personalized Offer Emails, Targeted Ads on social media, LinkedIn or Other Professional Platforms, Fake Events or Webinars, Targeted E-Commerce or Product Offers, Browsing Record-Based Phishing (Retargeting), Targeted Charity or Donation Campaigns, Surveys or Feedback Forms, Personalized WhatsApp or SMS Messages, and Use of Public Facts about Targets.
Vishing	Robocall or Malicious Call	Exclusive Promotional Offers by Phone, Fake Order Confirmations, Fake Charity or Donation Campaigns, Special Investment or Insurance Offers, Fake Surveys with Prizes, Customer Retention Scams, Lure of Prizes from social media or Online Contests, Confirmation of Changes to Customer Accounts or Data, Retargeting or Remarketing Based Scams, and Webinar or Online Event Registration Based Scams.
Baiting	Malicious USB Sticks or digital assets	Free Digital Content Promotions, Fake Giveaways, Fake Discounts or Coupons, Free E-Book or Educational Material Offers, Pop-Up Ads Offering Gifts or Services, Free Software or Plugin Offers, Fake "Try It Free" Campaigns, "Rare" or Exclusive File Promotions, Rewarded Surveys or Polls, and Rewarded QR Code Offers.
Smishing	The SMS contains a malicious link	Discount or Special Promo Offers, Order Confirmation or Package Delivery, Suspicious Activity Notifications on Accounts, Sweepstakes or Giveaway Winner Announcements, Surveys or Quizzes with Prizes, Service Upgrade Offers, Account Closure Announcements, Fake OTP Codes, Free Service Offers, and Personal Data Update Requests.
Water-Holing	Infected website with malicious code	Display Ads on Popular Sites, Manipulation of Affiliate or Partner Sites, Advertised Local Events or Events, and Attacks on Coupon or Discount Provider Sites.

Significantly few researchers have prevented social engineering attacks on digital marketing, such as preventing water-holing attacks by utilizing Remote Browser Isolation Technology [41] and building a Socio-Cyber-Physical System (SCPS) framework to protect digital marketing assets from the threat of cyber-attacks [39]. The study in [41] performs isolation and protection of website security access by utilizing Remote Browser Isolation Technology. The concept proposed by [41] helps maintain customer trust, ensure data privacy, and protect brand reputation in the ever-evolving digital marketing landscape. In contrast to [41], [39] combines social behavior analysis, physical network monitoring, and powerful artificial intelligence to build a comprehensive and flexible security system to identify cyber-attacks in advertisements, such as phishing.

There was no one-size-fits-all solution for social engineering attacks, and not all mitigation or defense strategies were equally effective for every target. Therefore, methods for identifying and addressing differences in each target and existing social engineering attack models were needed to develop better prevention strategies [35].

B. Information Security Policy

Existing information security policies proposed by various studies and defined based on correlation topics among the policy and other scope include:

1) General information security policy: To build and implement an information security policy, [42] identified ten necessary elements, namely risk assessment, policy construction, implementation, compliance, management, employee support, and three input elements for policy development, including policy guidance standards, drivers, and current literature related to information security policy. Different elements proposed by [42] and [43] design information security policy to prevent insider threats in organizations. The study uses six elements, namely cyber threat intelligence, organizational commitment, security intelligence, information security investment, and misperceptions of information security. Meanwhile, [44] formulated information security policy to assist in organizational regulation and information system security. Information security forms consist of three main elements, such as archives of main directions or policy, standard aspects or policy elements, and activity procedures or technical directions. Additionally, [45] identified determining elements of information security policy, including policy components, objectives, actionable tools, consequences, educational concepts, general concepts, and additional sources. Similar to [45], [46] used seven elements, namely local, global, and integration elements, areas of information security policy expertise, ISP characterization, management, and critical player factors to build an information security model.

The elements proposed by [46], [45], [42], [44], and [43] shared a common relationship. However, a crucial step or procedure is more critical in the development of an information security policy [47], [48], [49]. Action methods, incorporating planning, action, and reflection are used to formulate information security policy in Small and Medium Enterprise (SME). The planning phase comprises identifying SME problems, the action phase consists of formulating an information system security policy, and the reflection phase assesses whether the policy is consistent with organizational

goals and resolves SME problems. This method was different from that of [49], which deployed a framework to realize information security policy for higher education. To safeguard an educational organization information asset from internal, external, intentional, or unintentional threats, an "Information Security Policy" must be developed [50]. The phases for elaborating information security policy, according to [49], include team development as a pre-development process, risk assessment, regulation drafting, validated policy documents, as a process of development, realization, control, and evaluation of policy as a utilization process.

Various studies adopted different perspectives when developing information security policy, such as ontologies and models. [51] used four stages to analyze the ontology, defining policy recognition to determine permission, obligation, or prohibition rules for users, determining action rules for accessible options in the system, identifying compliance factors with policy, and determining actors and accessors or recipients of information security policy practices. In comparison with [51], [52] used a policy-and human-oriented model consisting of three main factors, namely information security policy awareness, security training, and computer and security technology proficiency. Differing from the model proposed by [52], [53] used a formal model to determine security policy in companies by adopting the Chinese wall concept. Similarly, [54] developed a finite automaton policy model for implementation in network security systems. Meanwhile, [55] proposed a model discussing motivation mechanisms for employees to comply with the Information Systems Security Policy (ISSP). While studies presented various models to determine information security policy, no evaluation has been conducted on the proposed models in developing policy.

Numerous studies tried to assess existing information security policy to optimize development. Reference [56] scrutinized information security policy for implementing e-commerce in Saudi Arabia, while [91] explored the phases, context, and content of ISP information security policy development. Adjusting information security policy with business strategies is crucial for successful implementation, as identified by [57], which explored the assimilation of information security policy using a normative, mimetic, and coercive method. Evaluation of information security policy across various sectors, including business environments [58], education [59], and multiple entities in different countries [60], showed considerations such as non-compliance, promotion, management, policy updates, and biased policy areas. Recommendations for information security policy stem from risk analysis, industry guidelines, government legislation, and current organizational policy, yet [60] showed a lack of consistency in applying 'security controls' across policy.

Despite numerous studies on information security policy, several critical aspects require improvement. This includes the adoption of proposed policy applicable to various organizations, countries, and conditions, the evaluation of awareness surrounding developed policy, the lack of evaluation for policy acceptance, and the absence of technical procedures accompanying policy implementation.

2) Information security policy in social engineering cases: Social engineering is a cyber-attack with significant repercussions for organizations and individuals and has received limited attention in the aspect of information security policy. Reference [61] evaluated social engineering victims and provided policy recommendations for affected organizations. The study suggested that while education is highly appropriate for individuals affected by social engineering attacks, it may not suffice for members of organizations facing repeated attacks. The need for more suitable sanctions for organizational members was also discussed, advocating for a policy-based method to prevent social engineering attacks.

3) Information security policy and formal model: Reference [62] constructed a formal verification for information flow security with dynamic policy in a system. Furthermore, the study developed a general security model incorporating dynamic security policy, underscoring the importance of considering security policy in securing the flow of information.

In summary, various studies established diverse information security policies across different domains and scopes. Generally, investigation on information security policy has been developed based on unique methods and study scopes. However, no prior explorations outlined a social engineering security policy model for digital marketing, which is a gap the current study aims to fill.

C. Risk Assessment in Security Policy

Conducting risk assessments is recommended as a foundational step in developing information security policy. Social engineering arises due to hackers exploiting human vulnerability [63]. Therefore, risk assessments are necessary for organizations and individuals as an initial step in formulating policy to prevent social engineering attacks. [63] identified the nature and key factors of social engineering, conducted a risk assessment using a probabilistic model, and subsequently implemented mitigation strategies based on the assessment results.

Compared with [63], [64] verified the attack vector and prevention of social engineering using a formal model method. Risk assessment models prove valuable in situations characterized by high uncertainty and known facts [64]. The developed risk assessment model aids decision-makers in choosing the optimal solution for mitigating vulnerability and reducing risks.

D. Information Security Policy Evaluation

Previous studies proposed evaluating information security policy. For example, [65] described information security policy measurement using the readability factor. The study used sequential mixed methods to assess the readability of information security policy, although it did not delve into explaining the elements of information security policy. Similar to prior investigations, this study does not evaluate social engineering policy for digital marketing. The current review aims to address the gap in the existing literature by exploring a

security policy model to prevent social engineering attacks in digital marketing, an area that has received limited attention.

The study topic primarily focused on social engineering and information security policy as shown in Table III. It was observed that there was an absence of a study topic specifically addressing social engineering policy for digital marketing. Reference [8] determined the connection between social engineering and marketing, showing that social engineering could be used to reach customers in marketing strategies. However, it could not be directly applied to prevent the impact of social engineering in marketing activities. Addressing these gaps would be interesting to develop a social engineering policy model for digital marketing.

TABLE III. COMPARISON OF THE REVIEW STUDIES

Years	Studies	Social engineering	Information security policy	Marketing/digital marketing
2022	[50]	-	√	-
2020	[66]	√	-	-
2022	[67]	√	-	-
2021	[68]	√	-	-
2021	[69]	√	-	-
2021	[20]	√	-	-
2020	[70]	√	-	-
2020	[71]	√	-	-
2020	[45]	-	√	-
2020	[72]	√	-	-
2022	[73]	√	-	-
2022	[60]	-	√	-
2022	[74]	-	√	-
2020	[57]	-	√	-
2024	This Study	√	√	√

III. METHODOLOGY

In this section, the research outlines the approach employed to formulate a security policy model aimed at preventing social engineering attacks within the domain of digital marketing. This analysis was organized following the findings presented in study [75]. The systematic and structured steps are outlined in three main stages, namely Planning, Conducting, and Reporting and Dissemination, as illustrated in Fig. 1.

In the planning phase, this research methodology was constructed based on the significant contributions found in this source. These references provide the theoretical foundation and key insights that guided the selection and evaluation of relevant articles. Therefore, the structure of this review acknowledges the significant contributions of this literature, which plays a critical role in shaping this study approach.

Moving into the conducting phases, this research involved a systematic and comprehensive exploration of the selected literature. This phase included a meticulous analysis of the identified articles to extract relevant information pertaining to the design and implementation of social engineering policy models in the realm of digital marketing. Data extraction methods were employed to categorize and synthesize key findings, enabling a detailed understanding of the methodologies, challenges, and outcomes presented in the literature. Additionally, during this phase, this research applied rigorous criteria to ensure the inclusion of studies that align closely with research question and objectives. The conducting phases were crucial in assembling a comprehensive overview of existing insights, paving the way for a nuanced and evidence-based evaluation of social engineering policy models in the context of digital marketing.

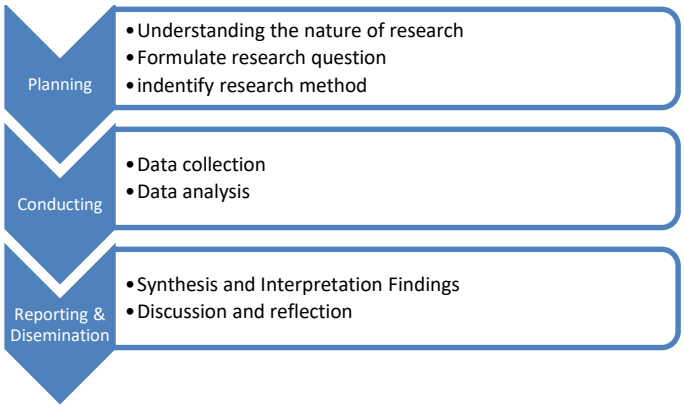

Fig. 1. The review study steps.

As this study transitioned into the reporting and dissemination phases, the focus shifted towards synthesizing the gathered information into a coherent narrative. This involved the compilation of a comprehensive report summarizing the key methodologies, findings, and insights obtained throughout the review. The report was structured to provide clarity and accessibility, ensuring that stakeholders and fellow researchers could easily comprehend the nuances of this study. Moreover, the dissemination aspect involved sharing research outcomes through appropriate channels, such as academic conferences, journals, and other platforms. This phase aimed to contribute to the broader scholarly conversation, fostering knowledge exchange and potentially influencing future research and practical applications in the field of social engineering policy models for digital marketing. Details of the criteria for the search, selection, and assessment process can be seen in Fig. 2.

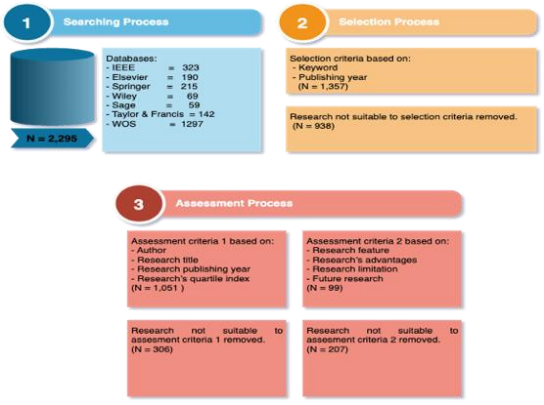

Fig. 2. Searching, Selection, and Assessment process.

A. Searching Process

The search process is a crucial component of this study, encompassing distinct selection and assessment phases. In the selection phase, the research objective was to identify and include studies that met predefined criteria essential to this study focus. Specific criteria, including aspects such as title, year of publication, and article type, were carefully applied to filter and include only studies relevant to this investigation.

To ensure a comprehensive exploration of the existing literature, the search was systematically conducted across nine renowned digital databases. These databases, namely ACM, Elsevier, Emerald, IEEE, Mdpi, Sage, Springer, Wiley, and the WOS index were selected for their prominence in hosting scholarly works related to the research domain. The inclusion of these diverse databases aimed to capture a broad spectrum of literature, enhancing the comprehensiveness and depth of this study.

Through this search process, this research sought to curate a robust collection of studies that would contribute meaningfully to understanding of social engineering policy models in the context of digital marketing. The emphasis on specific criteria and diverse databases ensures a rigorous and inclusive approach, allowing for a thorough examination of the available literature.

Aiming to address specific research question, "Which is the suitable method to design social engineering policy model for digital marketing?", this study identifies, elucidates, and summarizes suitable methods. Article selection is based on specific criteria with relevant keywords such as social engineering, information security policy, risk assessment, and evaluation methods.

The outcome of the search process revealed 2,295 articles, including 323 articles indexed by IEEE, 190 articles indexed by Elsevier, 215 indexed by Springer, 69 articles indexed by Wiley, 59 articles indexed by Sage, 142 articles indexed by Taylor & Francis, and 1,297 indexed by WOS.

B. Selection Process

To ensure the inclusion of studies aligned with the research objectives, a meticulous selection process was undertaken. Specific criteria were defined, centering on keywords deemed relevant to the investigation, including social engineering, information security policy, risk assessment, and evaluation. These keywords were strategically chosen to encapsulate the essential components of research focus, allowing us to narrow down the pool of potential studies.

This comprehensive selection approach, which spanned multiple databases and publishers, aimed to capture a representative sample of the available literature, enriching the breadth and depth of this study. By adhering to specific criteria and surveying various databases, this study sought to ensure a thorough and well-rounded examination of the relevant studies in the field of social engineering policy models for digital marketing.

Articles were screened using criteria related to keywords and publication year, resulting in the identification of 1,357 articles during this phase. However, 938 articles did not meet the specified selection criteria.

C. Assessment Process

The next step involved assessment process, which was the final stage in this study. The process identified studies that were consistent with the objectives of this current study, using specific criteria and context. Furthermore, a matrix was developed to capture essential information such as author, title, publication year, quartile index, features, advantages, limitations, and potential future research.

This study employed two sets of assessment criteria. The initial criteria screened articles according to authorship, research title, publication year, and quartile index, yielding a total of 1,051 articles meeting these criteria. However, 306 articles did not align with the first set of assessment criteria and were excluded. The second set of criteria evaluated articles based on research features, advantages, limitations, and future research, resulting in the identification of 99 articles meeting these criteria. Additionally, 207 articles were deemed unsuitable based on the second set of criteria and were consequently excluded.

As a result, the selection process yielded a diverse set of results from various databases. Specifically, this study retrieved 2 papers from ACM, 13 from Elsevier, 9 from Emerald, 45 from IEEE, 1 from MDPI, 2 from Sage, 13 from Springer, 3 from Wiley, and 11 from other publishers indexed by the Web of Science (WOS). The results are presented in Table IV, encompassing the number of selected articles from each database.

TABLE IV. RESULT ASSESSMENT PROCESS

Search String					
Databases	**Social Engineering**	**mation Security**	**k Assess**	**Evaluation Met**	
ACM	2	-	-	-	2
Elsevier	9	4	-	-	13
Emerald	6	3	-	-	9
IEEE	32	11	1	1	45
Mdpi	1	-	-	-	1
Sage	1	1	-	-	2
Springer	7	6	-	-	13
Wiley	3	-	-	-	3
WOS	6	4	1	-	11
	67	29	2	1	99

IV. RESULT

This study was categorized into three main areas with four subcategories, as shown in Table V. The primary contributions of the selected study for developing social engineering policy model for digital marketing comprised methods to building risk assessment based on qualitative methods models [63] or quantitative methods [64] and an evaluation method for information security policy before the release to users and stakeholders [76]. Finally, the selected study adopted different methods, aiming to develop information security policy or

prevent social engineering in the field of study, hence contributing to the development of a social engineering policy model for digital marketing.

TABLE V. MAPPING METHODOLOGY REVIEW

Methodology	Keyword	Study
Qualitative	Social Engineering	[7], [8], [18], [19], [29], [67], [68], [69], [70], [71], [72], [73], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116], [117], [118], [119], [120]
	Information Security Policy	[9], [15], [44], [45], [47], [48], [49], [51], [52], [54], [56], [57], [58], [59], [60], [62], [74], [121], [122], [123], [124]
	Risk Assessment	[63]
	Evaluation	-
Quantitative	Social Engineering	[125], [126], [127], [128], [129], [130], [131]
	Information Security Policy	[51], [132], [133]
	Risk Assessment	[64]
	Evaluation	[76]
Mix methods (Qualitative and Quantitative Methods)	Social Engineering	[66]
	Information Security Policy	[42], [43]
	Risk Assessment	-
	Evaluation	-

V. DISCUSSION

The previous studies offered recommendations for designing security policy model to prevent social engineering attacks in digital marketing. Although various methods existed for designing security policy models to prevent social engineering attacks, this current investigation, according to [57], followed three phases, namely identifying security policy requirements, developing security policy model, and validating security policy model.

However, previous ones fell short of comprehensively addressing all three phases of designing security policy models to prevent social engineering attacks. It should be acknowledged that each study tended to concentrate on a specific part. For example, [118] exclusively discussed the user-centric model without covering other phases of designing security policy model for preventing social engineering attacks in digital marketing. Meanwhile, it overlooked the phases of developing security policy models, risk assessment frameworks, formal methods, and evaluation methods. This implies that future works are needed to design a comprehensive approach to model security policies to prevent social engineering attacks in digital marketing and to implement them in various organizations to see the effectiveness of the policies.

This study experienced several limitations, including acquiring methods to evaluate social engineering attack policy, particularly before and after policy implementation. Several studies solely concentrated on building information security policies to counter information security threats. Additionally, some social engineering explorations were limited to evaluating perceptions about information security policy and using formal models to identify essential processes in information security policy. While readability methods served as an alternative for assessing policy effectiveness, challenges existed in determining how to assess better readability in an organizational context. The aspect of digital marketing for social engineering is relatively new, yet numerous social engineering activities inevitably occur, particularly in information gathering. Even though the term "social engineering" in marketing carries a positive connotation, when the activity deviates, it could cause a threat to digital marketing activities without realization.

VI. CONCLUSION

This review successfully identifies methodologies that can be used to build Social Engineering Policy Models, especially Digital Marketing. This review categorizes quality articles into three methodologies, namely Qualitative, Quantitative, and mixed methods. Each article is categorized into social engineering, information security policy, risk assessment, and evaluation. Based on the review's findings, many researchers only build policies to prevent social engineering attacks but do not validate the policies used, especially researchers who use mixed methods. Therefore, one of the directions of future research development is to ensure that every social engineering attack policy built must be validated or assessed. Validation and assessment can use formal methods and risk assessment techniques.

ACKNOWLEDGMENT

The authors also would like to show gratitude to Faculty of Information Science and Technology, and Universiti Kebangsaan Malaysia for their support.

REFERENCES

[1] European Union Agency For Network And Information Security, "Definition of Cybersecurity-Gaps and overlaps in standardisation," 2015. doi: 10.2824/4069.

[2] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines: revision 3," Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-63-3.

[3] Verizon, "DBIR 2023 Data Breach Investigations Report," 2023.

[4] Chen, Chiang, and Storey, "Business Intelligence and Analytics: From Big Data to Big Impact," MIS Quarterly, vol. 36, no. 4, p. 1165, 2012, doi: 10.2307/41703503.

[5] A. Kennedy and A. Parsons, "Macro-social marketing and social engineering: a systems approach," J Soc Mark, vol. 2, no. 1, pp. 37–51, Feb. 2012, doi: 10.1108/20426761211203247.

[6] J. Lies, "Marketing Intelligence and Big Data: Digital Marketing Techniques on their Way to Becoming Social Engineering Techniques in Marketing," International Journal of Interactive Multimedia and Artificial Intelligence, vol. 5, no. 5, pp. 134–144, 2019, doi: 10.9781/ijimai.2019.05.002.

[7] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," Journal of Information Security and Applications, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[8] A. M. Kennedy and A. Parsons, "Social engineering and social marketing: Why is one 'good' and the other 'bad'?," J Soc Mark, vol. 4, no. 3, pp. 198–209, Sep. 2014, doi: 10.1108/JSOCM-01-2014-0006.

[9] M. J. Magalhães, S. T. de Magalhães, K. Revett, and H. Jahankhani, "A review on privacy issues in hotels: A contribution to the definition of information security policies and marketing strategies," in Communications in Computer and Information Science, Springer Verlag, 2016, pp. 205–217. doi: 10.1007/978-3-319-51064-4_17.

[10] E. Stavrou, A. Piki, and P. Varnava, "Merging Policy and Practice: Crafting Effective Social Engineering Awareness-Raising Policies," in International Conference on Information Systems Security and Privacy, Science and Technology Publications, Lda, 2024, pp. 179–186. doi: 10.5220/0012410300003648.

[11] D. Singh, "Civil Servants Awareness Guideline Towards Computer Security Policy: A Case Study at the Manpower Department, Ministry of Human Resources," Asia-Pacific Journal of Information Technology and Multimedia, vol. 10, no. 01, pp. 86–99, Jun. 2021, doi: 10.17576/apjitm-2021-1001-08.

[12] J. O. Oyelami and A. M. Kassim, "Cyber Security Defence Policies: A Proposed Guidelines for Organisations Cyber Security Practices," 2020. [Online]. Available: www.ijacsa.thesai.org

[13] M. A. Pitchan and S. Z. Omar, "Cyber security policy: Review on netizen awareness and laws," Jurnal Komunikasi: Malaysian Journal of Communication, vol. 35, no. 1, pp. 103–119, 2019, doi: 10.17576/JKMJC-2019-3501-08.

[14] N. Rawindaran et al., "Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom," Digital, vol. 3, no. 3, pp. 200–231, Sep. 2023, doi: 10.3390/digital3030014.

[15] K. F. Steinmetz and T. J. Holt, "Falling for Social Engineering: A Qualitative Analysis of Social Engineering Policy Recommendations," Soc Sci Comput Rev, vol. 41, no. 2, pp. 592–607, Apr. 2023, doi: 10.1177/08944393221117501.

[16] N. A. Azam, A. Geogiana Buja, R. Ahmad, S. F. A. Latip, and N. M. Sahri, "An Analysis of the Deployment of Synergistic Cyber Security Awareness Model for the Elderly (SCSAM-Elderly) in Malaysia," Akademika, vol. 94, no. 3, pp. 90–107, 2024, doi: 10.17576/akad-2024-9403-06.

[17] H. A. Aldawood and G. Skinner, "A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications," in 2018 26th International Conference on Systems Engineering (ICSEng), IEEE, Dec. 2018, pp. 1–6. doi: 10.1109/ICSENG.2018.8638166.

[18] L. Pharris and B. Perez-Mira, "Preventing social engineering: a phenomenological inquiry," Information and Computer Security, vol. 31, no. 1, pp. 1–31, Feb. 2023, doi: 10.1108/ICS-09-2021-0137.

[19] K. Matyokurehwa, N. Rudhumbu, C. Gombiro, and C. Chipfumbu-Kangara, "Enhanced social engineering framework mitigating against social engineering attacks in higher education," SECURITY AND PRIVACY, vol. 5, no. 5, Sep. 2022, doi: 10.1002/spy2.237.

[20] B. Kotkova and M. Hromada, "Cyber Security and Social Engineering," in Proceedings - 25th International Conference on Circuits, Systems, Communications and Computers, CSCC 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 134–140. doi: 10.1109/CSCC53858.2021.00031.

[21] N. Cavdar Aksoy, E. Tumer Kabadayi, C. Yilmaz, and A. Kocak Alan, "A typology of personalisation practices in marketing in the digital age," Journal of Marketing Management, vol. 37, no. 11–12, pp. 1091–1122, 2021, doi: 10.1080/0267257X.2020.1866647.

[22] M. Schmitt and I. Flechais, "Digital deception: generative artificial intelligence in social engineering and phishing," Artif Intell Rev, vol. 57, no. 12, p. 324, Oct. 2024, doi: 10.1007/s10462-024-10973-2.

[23] K. Roethke, J. Klumpe, M. Adam, and A. Benlian, "Social influence tactics in e-commerce onboarding: The role of social proof and reciprocity in affecting user registrations," Decis Support Syst, vol. 131, Apr. 2020, doi: 10.1016/j.dss.2020.113268.

[24] A. Mollazehi, I. Abuelezz, M. Barhamgi, K. M. Khan, and R. Ali, "Do Cialdini's Persuasion Principles Still Influence Trust and Risk-Taking When Social Engineering is Knowingly Possible?," in Lecture Notes in Business Information Processing, vol. 513, Springer Science and Business Media Deutschland GmbH, 2024, pp. 273–288. doi: 10.1007/978-3-031-59465-6_17.

[25] V. Pavlidou, J. Otterbacher, and S. Kleanthous, "User Perception of Algorithmic Digital Marketing in Conditions of Scarcity," in Lecture Notes in Business Information Processing, Springer Science and Business Media Deutschland GmbH, 2022, pp. 319–332. doi: 10.1007/978-3-030-95947-0_22.

[26] M. A. Siddiqi, W. Pak, and M. A. Siddiqi, "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures," Jun. 01, 2022, MDPI. doi: 10.3390/app12126042.

[27] E. Sung, D. I. D. Han, Y. K. Choi, B. Gillespie, A. Couperus, and M. Koppert, "Augmented digital human vs. human agents in storytelling marketing: Exploratory electroencephalography and experimental studies," Psychol Mark, vol. 40, no. 11, pp. 2428–2446, Nov. 2023, doi: 10.1002/mar.21898.

[28] E. Dincelli and I. S. Chengalur-Smith, "Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling," European Journal of Information Systems, vol. 29, no. 6, pp. 669–687, 2020, doi: 10.1080/0960085X.2020.1797546.

[29] Y. Kano and T. Nakajima, "Trust factors of social engineering attacks on social networking services," in LifeTech 2021 - 2021 IEEE 3rd Global Conference on Life Sciences and Technologies, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 25–28. doi: 10.1109/LifeTech52111.2021.9391929.

[30] S. S. I. Rahim, M. I. Mohd Huda, S. Sa'ad, and R. Moorthy, "Cyber Security Crisis/Threat: Analysis of Malaysia National Security Council (NSC) Involvement Through the Perceptions of Government, Private and People Based on the 3P Model," e-Bangi Journal of Social Science and Humanities, vol. 21, no. 2, May 2024, doi: 10.17576/ebangi.2024.2102.17.

[31] S. Mamat, W. A. Wan Mahmud, and A. A. Azlan, "Trend Berkomunikasi dan Transaksi Dalam Talian: Selamatkah Data Peribadi Belia Malaysia?," e-Bangi Journal of Social Science and Humanities, vol. 20, no. 3, Aug. 2023, doi: 10.17576/ebangi.2023.2003.08.

[32] S. Waelchli and Y. Walter, "Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study," Comput Secur, vol. 148, Jan. 2025, doi: 10.1016/j.cose.2024.104137.

[33] P. M. W. Musuva, K. W. Getao, and C. K. Chepken, "A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility," Comput Human Behav, vol. 94, pp. 154–175, May 2019, doi: 10.1016/j.chb.2018.12.036.

[34] S. G. Abbas et al., "Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach," Sensors, vol. 21, no. 14, Jul. 2021, doi: 10.3390/s21144816.

[35] M. Aijaz and M. Nazir, "Modelling and analysis of social engineering threats using the attack tree and the Markov model," International Journal of Information Technology (Singapore), vol. 16, no. 2, pp. 1231–1238, Feb. 2024, doi: 10.1007/s41870-023-01540-z.

[36] A. H. Shakiba, G. Ghadiri, and H. S. Karaki, "Iran's Legislative Policy in dealing with Fraud During COVID-19 Pandemic," JURNAL UNDANG-UNDANG DAN MASYARAKAT, vol. 33, pp. 103–118, Dec. 2023, doi: 10.17576/juum-2023-33-09.

[37] A. Rodrigues, M. L. B. Villela, and E. L. Feitosa, "Privacy Threat MOdeling Language," IEEE Access, vol. 11, pp. 24448–24471, 2023, doi: 10.1109/ACCESS.2023.3255548.

[38] F. Fkih and G. Al-Turaif, "Threat Modelling and Detection Using Semantic Network for Improving Social Media Safety," International Journal of Computer Network and Information Security, vol. 15, no. 1, pp. 39–53, Feb. 2023, doi: 10.5815/ijcnis.2023.01.04.

[39] S. Yang and H. Long, "Socio Cyber-Physical System for Cyber-Attack Detection in Brand Marketing Communication Network," Wirel Pers Commun, Jun. 2024, doi: 10.1007/s11277-024-11261-6.

[40] 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, Dec. 2021, doi: 10.1186/s42400-021-00094-6.

[41] J. Hu, H. Wang, and Y. Liu, "Strengthening Digital Marketing Security Website Threat Isolation and Protection Using Remote Browser Isolation Technology," Comput Aided Des Appl, pp. 56–74, Nov. 2023, doi: 10.14733/cadaps.2024.s4.56-74.

[42] S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," Comput Secur, vol. 61, pp. 169–183, Aug. 2016, doi: 10.1016/j.cose.2016.06.002.

[43] H. Stewart, "A systematic framework to explore the determinants of information security policy development and outcomes," Information and Computer Security, vol. 30, no. 4, pp. 490–516, Oct. 2022, doi: 10.1108/ICS-06-2021-0076.

[44] E. L. G. Fontes and A. J. Balloni, "Information security policy: The regulatory basis for the protection of information systems," in Laboratory Management Information Systems: Current Requirements and Future Perspectives, IGI Global, 2014, pp. 95–117. doi: 10.4018/978-1-4666-6320-6.ch006.

[45] E. Rostami, F. Karlsson, and S. Gao, "Requirements for computerized tools to design information security policies," Comput Secur, vol. 99, Dec. 2020, doi: 10.1016/j.cose.2020.102063.

[46] A. Klaic and M. Golub, "Conceptual information modelling within the contemporary information security policies," 2013.

[47] I. Lopes and P. Oliveira, "Implementation of information systems security policies: A survey in small and medium sized enterprises," in Advances in Intelligent Systems and Computing, Springer Verlag, 2015, pp. 459–468. doi: 10.1007/978-3-319-16486-1_45.

[48] I. Lopes and P. Oliveira, "Applying action research in the formulation of information security policies," in Advances in Intelligent Systems and Computing, Springer Verlag, 2015, pp. 513–522. doi: 10.1007/978-3-319-16486-1_50.

[49] W. B. W. Ismail, S. Widyarto, R. A. T. R. Ahmad, and K. A. Ghani, "A generic framework for information security policy development," in 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), IEEE, Sep. 2017, pp. 1–6. doi: 10.1109/EECSI.2017.8239132.

[50] P. Petrov, I. Kuyumdzhiev, R. Malkawi, G. Dimitrov, and J. Jordanov, "Digitalization of Educational Services with Regard to Policy for Information Security," TEM Journal, vol. 11, no. 3, pp. 1093–1102, Aug. 2022, doi: 10.18421/TEM113-14.

[51] D. Mandal and C. Mazumdar, "Towards an ontology for enterprise level information security policy analysis," in ICISSP 2021 - Proceedings of the 7th International Conference on Information Systems Security and Privacy, SciTePress, 2021, pp. 492–499. doi: 10.5220/0010248004920499.

[52] K. E. H. A. Alhosani, S. K. A. Khalid, N. A. Samsudin, S. Jamel, and K. M. bin Mohamad, "A policy driven, human oriented information security model: a case study in UAE banking sector," in 2019 IEEE Conference on Application, Information and Network Security (AINS), IEEE, Nov. 2019, pp. 12–17. doi: 10.1109/AINS47559.2019.8968705.

[53] T. Y. T. Y. Lin, "Chinese wall security policies information flows in business cloud," in Proceedings - 2015 IEEE International Conference on Big Data, IEEE Big Data 2015, Institute of Electrical and Electronics Engineers Inc., Dec. 2015, pp. 1603–1607. doi: 10.1109/BigData.2015.7363927.

[54] D. Chernyavskiy and N. Miloslavskaya, "An Approach to Information Security Policy Modeling for Enterprise Networks," in Communications and Multimedia Security, B. De Decker and A. Zúquete, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 118–127.

[55] H. P. Shih, X. Guo, K. H. Lai, and T. C. E. Cheng, "Taking promotion and prevention mechanisms matter for information systems security policy in Chinese SMEs," in Proceedings of 2016 International Conference on Information Management, ICIM 2016, Institute of Electrical and Electronics Engineers Inc., May 2016, pp. 110–115. doi: 10.1109/INFOMAN.2016.7477543.

[56] K. Thakur, M. L. Ali, K. Gai, and M. Qiu, "Information Security Policy for E-Commerce in Saudi Arabia," in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), IEEE, Apr. 2016, pp. 187–190. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.14.

[57] H. Paananen, M. Lapke, and M. Siponen, "State of the art in information security policy development," Jan. 01, 2020, Elsevier Ltd. doi: 10.1016/j.cose.2019.101608.

[58] M. Alotaibi, S. Furnell, and N. Clarke, "Information security policies: A review of challenges and influencing factors," in 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, Institute of Electrical and Electronics Engineers Inc., Feb. 2017, pp. 352–358. doi: 10.1109/ICITST.2016.7856729.

[59] L. G. Ording, S. Gao, and W. Chen, "The influence of inputs in the information security policy development: an institutional perspective," Transforming Government: People, Process and Policy, vol. 16, no. 4, pp. 418–435, Oct. 2022, doi: 10.1108/TG-03-2022-0030.

[60] B. Ngoqo and K. Njenga, "The state of e-Government security in South Africa: Analysing the national information security policy," in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Springer Verlag, 2018, pp. 29–46. doi: 10.1007/978-3-319-98827-6_3.

[61] K. F. Steinmetz, T. J. Holt, and C. G. Brewer, "Developing and implementing social engineering-prevention policies: a qualitative study," Security Journal, Jun. 2023, doi: 10.1057/s41284-023-00385-2.

[62] J. Sun, X. Long, and Y. Zhao, "A Verified Capability-Based Model for Information Flow Security With Dynamic Policies," IEEE Access, vol. 6, pp. 16395–16407, Mar. 2018, doi: 10.1109/ACCESS.2018.2815766.

[63] T. Li, K. Wang, and J. Horkoff, "Towards effective assessment for social engineering attacks," in Proceedings of the IEEE International Conference on Requirements Engineering, IEEE Computer Society, Sep. 2019, pp. 392–397. doi: 10.1109/RE.2019.00051.

[64] A. Şandor, G. Tont, and E. Simion, "A Mathematical Model for Risk Assessment of Social Engineering Attacks," TEM Journal, vol. 11, no. 1, pp. 334–338, Feb. 2022, doi: 10.18421/TEM111-42.

[65] Y. Alkhurayyif and G. R. S. Weir, "Readability as a basis for information security policy assessment," in 2017 Seventh International Conference on Emerging Security Technologies (EST), IEEE, Sep. 2017, pp. 114–121. doi: 10.1109/EST.2017.8090409.

[66] L. Bošnjak and B. Brumen, "Shoulder surfing experiments: A systematic literature review," Dec. 01, 2020, Elsevier Ltd. doi: 10.1016/j.cose.2020.102023.

[67] J. E. McNealy, "Platforms as phish farms: Deceptive social engineering at scale," New Media Soc, vol. 24, no. 7, pp. 1677–1694, Jul. 2022, doi: 10.1177/14614448221099228.

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

[69] M. Mattera and M. M. Chowdhury, "Social Engineering: The Looming Threat," in IEEE International Conference on Electro Information Technology, IEEE Computer Society, May 2021, pp. 56–61. doi: 10.1109/EIT51626.2021.9491884.

[70] A. Yasin, R. Fatima, L. Liu, J. Wang, and R. Ali, "Understanding Social Engineers Strategies from the Perspective of Sun-Tzu Philosophy," in Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020, Institute of Electrical and Electronics Engineers Inc., Jul. 2020, pp. 1773–1776. doi: 10.1109/COMPSAC48688.2020.00045.

[71] M. R. Arabia-Obedoza, G. Rodriguez, A. Johnston, F. Salahdine, and N. Kaabouch, "Social Engineering Attacks A Reconnaissance Synthesis Analysis," in 2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 0843–0848. doi: 10.1109/UEMCON51285.2020.9298100.

[72] K. S. Jones, M. E. Armstrong, M. K. Tornblad, and A. Siami Namin, "How social engineers use persuasion principles during vishing attacks," Information and Computer Security, vol. 29, no. 2, pp. 314–331, 2020, doi: 10.1108/ICS-07-2020-0113.

[73] W. Fuertes et al., "Impact of Social Engineering Attacks: A Literature Review," in Smart Innovation, Systems and Technologies, Springer

Science and Business Media Deutschland GmbH, 2022, pp. 25–35. doi: 10.1007/978-981-16-4884-7_3.

[74] N. M. C. Galego, R. M. Pascoal, and P. R. Brandao, "BYOD : Impact in Architecture and Information Security Corporate Policy," in 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, Jun. 2022, pp. 1–2. doi: 10.23919/CISTI54924.2022.9820043.

[75] A. Bryman and E. Bell, Business Research Methods. Oxford University Press, 2015. [Online]. Available: https://books.google.com.my/books?id=l7u6BwAAQBAJ

[76] Y. Alkhurayyif and G. R. S. Weir, "Evaluating Readability as a Factor in Information Security Policies," International Journal of Trend in Research and Development, pp. 20–22, 2017, Accessed: Aug. 25, 2024. [Online]. Available: https://strathprints.strath.ac.uk/id/eprint/63070

[77] T. Koide, D. Chiba, M. Akiyama, K. Yoshioka, and T. Matsumoto, "To get lost is to learn the way: An analysis of multi-step social engineering attacks on the web," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E104A, no. 1, pp. 162–181, Jan. 2021, doi: 10.1587/transfun.2020CIP0005.

[78] N. Tsinganos, P. Fouliras, G. Sakellariou, and I. Mavridis, "Towards an automated recognition system for chat-based social engineering attacks in enterprise environments," in ACM International Conference Proceeding Series, Association for Computing Machinery, Aug. 2018. doi: 10.1145/3230833.3233277.

[79] T. Nelms, R. Perdisci, M. Antonakakis, and M. Ahamad, "Towards measuring and mitigating social engineering software download attacks," in Proceedings of the 25th USENIX Conference on Security Symposium, in SEC'16. USA: USENIX Association, 2016, pp. 773–789.

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

[81] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analysing online social engineering attack surfaces," Comput Secur, vol. 69, pp. 18–34, Aug. 2017, doi: 10.1016/j.cose.2016.12.013.

[82] H. Wilcox and M. Bhattacharya, "A framework to mitigate social engineering through social media within the enterprise," in Proceedings of the 2016 IEEE 11th Conference on Industrial Electronics and Applications, ICIEA 2016, Institute of Electrical and Electronics Engineers Inc., Oct. 2016, pp. 1039–1044. doi: 10.1109/ICIEA.2016.7603735.

[83] V. M. I. A. Hartl and U. Schmuntzsch, "Fraud protection for online banking: A user-centered approach on detecting typical double-dealings due to social engineering and inobservance whilst operating with personal login credentials," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 2016, pp. 37–47. doi: 10.1007/978-3-319-39381-0_4.

[84] A. Jamil, K. Asif, Z. Ghulam, M. K. Nazir, S. Mudassar Alam, and R. Ashraf, "MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook," in 2018 IEEE International Conference on Big Data (Big Data), IEEE, Dec. 2018, pp. 5040–5048. doi: 10.1109/BigData.2018.8622505.

[85] H. Aldawood and G. Skinner, "Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions," IEEE Access, vol. 8, pp. 67321–67329, 2020, doi: 10.1109/ACCESS.2020.2983280.

[86] F. Goodarzian, P. Ghasemi, V. Kumar, and A. Abraham, "A new modified social engineering optimizer algorithm for engineering applications," Soft comput, vol. 26, no. 9, pp. 4333–4361, May 2022, doi: 10.1007/s00500-022-06837-y.

[87] R. Heartfield and G. Loukas, "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks," ACM Comput Surv, vol. 48, no. 3, pp. 1–39, Feb. 2016, doi: 10.1145/2835375.

[88] C. Atwell, T. Blasi, and T. Hayajneh, "Reverse TCP and Social Engineering Attacks in the Era of Big Data," in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), IEEE, Apr. 2016, pp. 90–95. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.60.

[89] Z. Wang, L. Sun, and H. Zhu, "Defining Social Engineering in Cybersecurity," IEEE Access, vol. 8, pp. 85094–85115, 2020, doi: 10.1109/ACCESS.2020.2992807.

[90] A. Algarni, Y. Xu, and T. Chan, "Social engineering in social networking sites: The art of impersonation," in Proceedings - 2014 IEEE International Conference on Services Computing, SCC 2014, Institute of Electrical and Electronics Engineers Inc., Oct. 2014, pp. 797–804. doi: 10.1109/SCC.2014.108.

[91] S. Uebelacker and S. Quiel, "The social engineering personality framework," in Proceedings - 4th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2014 - Co-located with 27th IEEE Computer Security Foundations Symposium, CSF 2014 in the Vienna Summer of Logic 2014, Institute of Electrical and Electronics Engineers Inc., Dec. 2014, pp. 24–30. doi: 10.1109/STAST.2014.12.

[92] I. Del Pozo, M. Iturralde, and F. Restrepo, "Social engineering: Application of psychology to information security," in Proceedings - 2018 IEEE 6th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2018, Institute of Electrical and Electronics Engineers Inc., Oct. 2018, pp. 108–114. doi: 10.1109/W-FiCloud.2018.00023.

[93] F. Mouton, L. Leenen, and H. S. Venter, "Social Engineering Attack Detection Model: SEADMv2," in Proceedings - 2015 International Conference on Cyberworlds, CW 2015, Institute of Electrical and Electronics Engineers Inc., Feb. 2015, pp. 216–223. doi: 10.1109/CW.2015.52.

[94] A. Yasin, R. Fatima, L. Liu, J. Wang, R. Ali, and Z. Wei, "Understanding and deciphering of social engineering attack scenarios," Security and Privacy, vol. 4, no. 4, Jul. 2021, doi: 10.1002/spy2.161.

[95] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, "Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble?," IEEE Robot Autom Lett, vol. 3, no. 4, pp. 3701–3708, Oct. 2018, doi: 10.1109/LRA.2018.2856272.

[96] A. Cullen and L. Armitage, "The social engineering attack spiral (SEAS)," in 2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016, Institute of Electrical and Electronics Engineers Inc., Jun. 2016. doi: 10.1109/CyberSecPODS.2016.7502347.

[97] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an Ontological Model Defining the Social Engineering Domain," 2014, pp. 266–279. doi: 10.1007/978-3-662-44208-1_22.

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

[99] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference, Institute of Electrical and Electronics Engineers Inc., Nov. 2014. doi: 10.1109/ISSA.2014.6950510.

[100] C. Lekati, "Complexities in Investigating Cases of Social Engineering: How Reverse Engineering and Profiling can Assist in the Collection of Evidence," in Proceedings - 11th International Conference on IT Security Incident Management and IT Forensics, IMF 2018, Institute of Electrical and Electronics Engineers Inc., Oct. 2018, pp. 107–109. doi: 10.1109/IMF.2018.00015.

[101] P. Burda, L. Allodi, and N. Zannone, "Dissecting Social Engineering Attacks through the Lenses of Cognition," in Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021, Institute of Electrical and Electronics Engineers Inc., Sep. 2021, pp. 149–160. doi: 10.1109/EuroSPW54576.2021.00024.

[102] A. Zingerle, "How to obtain passwords of online scammers by using social engineering methods," in Proceedings - 2014 International Conference on Cyberworlds, CW 2014, Institute of Electrical and Electronics Engineers Inc., Dec. 2014, pp. 340–344. doi: 10.1109/CW.2014.54.

[103] N. Tsinganos, I. Mavridis, and D. Gritzalis, "Utilizing Convolutional Neural Networks and Word Embeddings for Early-Stage Recognition of

Persuasion in Chat-Based Social Engineering Attacks," IEEE Access, vol. 10, pp. 108517–108529, 2022, doi: 10.1109/ACCESS.2022.3213681.

[104]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, doi: 10.1109/ACCESS.2016.2616285.

[105]A. Algarni, Y. Xu, and T. Chan, "Measuring source credibility of social engineering attackers on Facebook," in Proceedings of the Annual Hawaii International Conference on System Sciences, IEEE Computer Society, Mar. 2016, pp. 3686–3695. doi: 10.1109/HICSS.2016.460.

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

[107]E. U. Osuagwu, G. A. Chukwudebe, T. Salihu, and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity," in CYBER-Abuja 2015 - International Conference on Cyberspace Governance: The Imperative for National and Economic Security - Proceedings, Institute of Electrical and Electronics Engineers Inc., Dec. 2015, pp. 91–100. doi: 10.1109/CYBER-Abuja.2015.7360515.

[108]P. Schaab, K. Beckers, and S. Pape, "Social engineering defence mechanisms and counteracting training strategies," 2017, Emerald Group Publishing Ltd. doi: 10.1108/ICS-04-2017-0022.

[109]J. W. Bullee and M. Junger, "How effective are social engineering interventions? A meta-analysis," Nov. 04, 2020, Emerald Group Holdings Ltd. doi: 10.1108/ICS-07-2019-0078.

[110]N. Abe and M. Soltys, "Deploying Health Campaign Strategies to Defend Against Social Engineering Threats," Procedia Comput Sci, vol. 159, pp. 824–831, 2019, doi: 10.1016/j.procs.2019.09.241.

[111]C. C. Campbell, "Solutions for counteracting human deception in social engineering attacks," Information Technology and People, vol. 32, no. 5, pp. 1130–1152, Sep. 2019, doi: 10.1108/ITP-12-2017-0422.

[112]F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," 2019, MDPI AG. doi: 10.3390/FI11040089.

[113]H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon, "Mind your SMSes: Mitigating Social Engineering in Second Factor Authentication," 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740481630116X

[114]F. Mouton, A. Nottingham, L. Leenen, and H. S. Venter, "Finite State Machine for the Social Engineering Attack Detection Model: SEADM," SAIEE Africa Research Journal, vol. 109, no. 2, pp. 133–148, Jun. 2018, doi: 10.23919/SAIEE.2018.8531953.

[115]R. J. Heartfield, "Utilising the concept of human-as-a-security-sensor for detecting semantic social engineering attacks," PhD thesis, University of Greenwich, 2017.

[116]A. Algarni, "Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models," International Journal of e-Education, e-Business, e-Management and e-Learning, 2013, doi: 10.7763/IJEEEE.2013.V3.278.

[117]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, doi: 10.1016/j.cose.2018.02.020.

[118]S. Albladi and G. R. S. Weir, "Vulnerability to social engineering in social networks: a proposed user-centric framework," in 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), IEEE, Jun. 2016, pp. 1–6. doi: 10.1109/ICCCF.2016.7740435.

[119]D. Al-dablan, A. Al-hamad, R. Al-Bahlal, and M. Altaib Badawi, "An Analysis of Various Social Engineering Attack in Social Network using Machine Learning Algorithm," IJCSNS International Journal of Computer Science and Network Security, vol. 20, no. 10, p. 46, 2020, doi: 10.22937/IJCSNS.2020.20.10.7.

[120]N. Mamedova, A. Urintsov, O. Staroverova, E. Ivanov, and D. Galahov, "Social engineering in the context of ensuring information security," SHS Web of Conferences, vol. 69, p. 00073, 2019, doi: 10.1051/shsconf/20196900073.

[121]R. Anand, S. Medhavi, V. Soni, C. Malhotra, and D. K. Banwet, "Transforming information security governance in India (A SAP-LAP based case study of security, IT policy and e-governance)," Information and Computer Security, vol. 26, no. 1, pp. 58–90, 2018, doi: 10.1108/ICS-12-2016-0090.

[122]S. K. Jansen van Rensburg, "End-User Perceptions on Information Security," Journal of Global Information Management, vol. 29, no. 6, pp. 1–16, Dec. 2021, doi: 10.4018/JGIM.293290.

[123]E. Rostami, F. Karlsson, and S. Gao, "Policy Components - A Conceptual Model for Tailoring Information Security Policies," in IFIP Advances in Information and Communication Technology, Springer Science and Business Media Deutschland GmbH, 2022, pp. 265–274. doi: 10.1007/978-3-031-12172-2_21.

[124]M. Kang, T. Lee, and S. Um, "Establishment of Methods for Information Security System Policy Using Benchmarking," in Proceedings - 29th IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2018, Institute of Electrical and Electronics Engineers Inc., Nov. 2018, pp. 237–242. doi: 10.1109/ISSREW.2018.00012.

[125]T. Grassegger and D. Nedbal, "The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering," Procedia Comput Sci, vol. 181, pp. 59–66, 2021, doi: 10.1016/j.procs.2021.01.103.

[126]F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," in Proceedings - IEEE Symposium on Security and Privacy, Institute of Electrical and Electronics Engineers Inc., Nov. 2014, pp. 236–250. doi: 10.1109/SPW.2014.39.

[127]S. Vrhovec, I. Bernik, and B. Markelj, "Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign," Comput Secur, vol. 125, Feb. 2023, doi: 10.1016/j.cose.2022.103038.

[128]S. M. Albladi and G. R. S. Weir, "Predicting individuals' vulnerability to social engineering in social networks," Cybersecurity, vol. 3, no. 1, Dec. 2020, doi: 10.1186/s42400-020-00047-5.

[129]N. Wulandari, M. S. Adnan, and C. B. Wicaksono, "Are You a Soft Target for Cyber Attack? Drivers of Susceptibility to Social Engineering-Based Cyber Attack (SECA): A Case Study of Mobile Messaging Application," Hum Behav Emerg Technol, vol. 2022, 2022, doi: 10.1155/2022/5738969.

[130]A. Algarni, "What message characteristics make social engineering successful on Facebook: The role of central route, peripheral route, and perceived risk," Information (Switzerland), vol. 10, no. 6, Jun. 2019, doi: 10.3390/info10060211.

[131]L. Karadsheh, H. Alryalat, J. Alqatawna, S. F. Alhawari, and M. A. AL Jarrah, "The impact of social engineer attack phases on improved security countermeasures: Social engineer involvement as mediating variable," International Journal of Digital Crime and Forensics, vol. 14, no. 1, pp. 1–26, Jan. 2022, doi: 10.4018/IJDCF.286762.

[132]K. P. Gallagher, X. Zhang, and V. C. Gallagher, "Institutional drivers of assimilation of information security policies and procedures in U.S. firms: Test of an empirical model," in Proceedings of the Annual Hawaii International Conference on System Sciences, IEEE Computer Society, Mar. 2015, pp. 4700–4709. doi: 10.1109/HICSS.2015.559.

[133]S. Solak and Y. Zhuo, "Optimal policies for information sharing in information system security," Eur J Oper Res, vol. 284, no. 3, pp. 934–950, Aug. 2020, doi: 10.1016/j.ejor.2019.12.016.