Hindawi
Human Behavior and Emerging Technologies
Volume 2022, Article ID 5738969, 10 pages
https://doi.org/10.1155/2022/5738969

Research Article

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

Nuri Wulandari, Mohammad Syauqi Adnan, and Chastio Bayu Wicaksono

Indonesia Banking School, Kemang Raya 35, Jakarta, Indonesia 12730

Correspondence should be addressed to Nuri Wulandari; nuri.w.h@ibs.ac.id

Received 1 August 2022; Revised 11 November 2022; Accepted 14 November 2022; Published 7 December 2022

Academic Editor: Zheng Yan

A rise in working and studying from home, activities which depend on the Internet, and the exchange of data coupled with a lack of understanding about security for interacting in cyberspace have made cybersecurity one of the most pressing concerns today. One form, in particular, is a social engineering-based cyber attack. Unfortunately, not much research has been conducted on the susceptibility factors that cause this to happen. This study attempts to understand what factors make a person susceptible to cyber attacks that can be seen from three perspectives: habitual perspective, perception perspective, and social and motivation perspective. The objective of the research is to identify specific characteristics and drivers regarding the social engineering-based cyber attack (SECA) susceptibility of a consumer exposed to social media messaging applications. A quantitative survey was employed to test a total of 114 respondents in Indonesia who are categorized as active Internet users. The study found variables within two of the three perspectives that positively contributed to a consumer's susceptibility to cyberattack. These factors will provide valuable insight into prevention and knowledge of related risks of cyberattacks based on social engineering in the future.

1. Introduction

Due to the COVID-19 pandemic and large-scale restrictions imposed in almost all countries around the world, working and schooling from home has become the new norm. The migration of activities to the online platform is changing people's approach to everyday activities. Teleworking has increased tremendously with the pandemic as a method for companies to adapt to the situation [1]. Thus, individuals and organizations are becoming increasingly dependent on the Internet to carry out their daily work. This has resulted in a huge increase in virtual presence and time spent online [2]. In line with the increasing interactions in cyberspace, the potential risk of cyber attack posed by these specific changes in behavior during the pandemic is increasing globally [3, 4]. The psychological anxiety and fear that people experienced during the pandemic actually drove the success of cyberattack incidence [5]. These conditions make cybersecurity one of the most significant issues today. Protecting people and organizations from becoming targets for cybercriminals is a priority for industry and academia [6].

Cybersecurity attacks increased 600% during the pandemic [7]. Nearly all of the world's regions are affected by cyber threats, including the Asia-Pacific region. In fact, Asia was the most targeted region for cyber attacks in 2021, accounting for one in every four attacks worldwide, or 26% [8]. Specifically, in Indonesia, where this study is based, the National Cyber and Crypto Agency recorded an extraordinary number of cyber attacks during 2020. As of August 2020, there were 189 million; however, by November 2020, the total was 423 million attacks. In cases of data breach, during the period from January to August 2020, there were 36,771 data accounts stolen in a number of sectors, including the financial sector. A survey from Palo Alto [9] stated that the biggest challenges of Indonesian cybersecurity are outdated infrastructure and lack of awareness, especially from the public, who have not been made aware of the importance of maintaining security even in the individual sphere.

Cybersecurity threats manifest in many ways. Primary methods of cybersecurity attack include phishing, ransomware, cryptojacking, data breach, malware, disinformation, and other nonmalicious threats. Most of the attacks require technical skills to orchestrate; however, there are also threats that utilize individual weaknesses. One of the most widely used techniques to commit crimes which focus on individual susceptibility is called Social Engineering. The most common attacks, such as phishing, use the techniques of Social Engineering [10]. Social Engineering strategies deceive victims by taking data that are important for access to financial or other data by exploiting the trust, motives, habits, and behavior of individuals to manipulate them [11, 12].

Social engineering has emerged as a serious threat in virtual communities and is an effective way to attack information systems [13]. It is considered to be the most effective technique for attacking even the most secure system, since the weakest link of any system is the users [14]. It is one of the highest risks among other threats such as identity theft, key logger, and cyberbullying [15]. Unfortunately, not much has been learned about the factors that cause this to happen [16]. The literature suggests that future study needs to be conducted to analyze factors influencing social engineering susceptibility [17].

The study's objectives are to identify the characteristic and behavioral drivers that influence susceptibility of social engineering-based cyber attack (SECA). It aims to fill the gap by measuring the level of people's susceptibility to the threat of cybersecurity attacks based on social engineering methods, specifically in relation to social media messaging applications. The issue will be investigated from three different perspectives that can influence cyber attack susceptibility based on previous research by Albladi and Weir [18], with modification of scenarios to adapt to social media messaging applications. Data from Statista (2022) revealed that there many mobile messaging applications as of January 2022. Based on the number of monthly active users, WhatsApp is ranked first, with 2 billion users, followed by WeChat, Facebook Messenger, QQ, Snapchat, and Telegram. Accordingly, the study is limited to the most popular mobile messaging application brand, WhatsApp.

2. Methods

The study employed a quantitative method using questionnaires which were prepared beforehand with an interview with an expert. There are two steps involved in the process. The first is the development of susceptibility scenarios, and the second is the questionnaire survey. The susceptibility variable is measured by presenting the scenarios of a cyberattack situation and measuring an interviewee's responses. After a careful review of the initial scenarios from Albladi and Weir [18], for the study, we decided to develop a new set of scenarios based on discussion with cybersecurity experts. This new set of scenarios is more relevant to the mobile messaging application and validated by an expert. The next step was to incorporate the scenarios into a quantitative survey with a unit of analysis of students and/or productive employees.

Interviews were conducted with cybersecurity experts. The aim was to confirm the initial scenario by Albladi and Weir [18]. The expert indicated that the scenarios were not relevant for the context of the study, thus suggesting finding new scenarios for a mobile messaging application context. The research team then curated several scenarios from the media reporting social engineering-based cyber attacks in mobile messaging application contexts.

The scenarios consisted of three types of cyber attack: phishing, clickjacking, and malware. The scenario sets were designed to accommodate at least 6 scenarios with different levels of risk: high, medium, and low. The risk level was set based on the consultation with a cybersecurity expert. These scenarios were part of the survey questions for susceptibility variables that were asked in part 2. Respondents were presented with the scenarios and asked how likely they were to perform the action requested by each scenario. The measurement ranges from 1 for "Never" to 5 for "Definitely". The final development of the scenarios and instruction used in this study is provided in Table 1.

The questionnaire survey was conducted with an analysis unit of students and/or young productive employees who actively use the Internet to study and work in big cities in Indonesia. Data were collected with a total target of 114 respondents and then analyzed with the help of the SmartPLS statistical tool. In taking the sample, the authors used a nonprobability sampling method, a type of convenience sampling.

2.1. Literature Review

2.1.1. Social Engineering-Based Cyber Attack (SECA). A definition of social engineering according to Mitnick and Simon [12] is all the effort to manipulate a victim's motives, habits, and behavior. The effort requires direct or indirect social interaction between the attacker and victim [19]. Several definitions using interaction as the basis of initiating the attack include Mouton et al. [20], who defined social engineering as a science of using social interaction in order to persuade an individual or organization to perform a specific request. This request might employ one or more methods of social engineering, indirect or direct communication, a target, medium, goal, and principles of compliance. Boshmaf et al. [21] described social engineering as a form of art to gain access to an otherwise secure object by exploiting human psychology. This definition highlights the importance of psychological and behavioral discipline in the method of social engineering. The psychological term that is most commonly used in the definition of social engineering is manipulation. Breda et al. [22] stated that social engineering is the design and application of techniques in order to deliberately manipulate humans. In a cybersecurity context, this technique is used to lure victims in order to disclose confidential data or breach other security protocols including infecting the system and releasing classified information.

The basic classification of SECA consists of human-based attacks and technology-based attacks [11, 23]. There are three methods of attack that can be conducted: social,

Table 1: Susceptibility instruction and scenarios. Instructions: read carefully the scenario below. Each scenario describes a situation that commonly occurs when we surf in cyberspace. You are asked to state the action or reaction you are most likely to take when faced with the scenario. The reaction that is measured is the likelihood that you will carry out the desired follow up in the scenario; it can be in the form of filling in the data or clicking the next button. Your honesty when filling out our survey is very helpful, and there are no right or wrong answers in each of these situations.

Type of attack and risk level	Scenarios	Next action (1 = never, 2 = not likely, 3 = maybe, 4 = most likely, 5 = definitely)
Scenario 1 (Q7_1) Clickjacking Risk level: medium	Sensational greetings, win millions of rupiah on the biggest and most trusted website, click now: http://www.joinhoki21boxq.com to get attractive bonuses.	How likely are you to do what the page asks you to do?
Scenario 2 (Q7_2) Phising Risk level: high	Hello, I am an employee of Shopx pay Indonesia. You get a gift in the form of Shopx pay in the amount of 1 million rupiah. We need a Shopx pay pin and a verification code (OTP).	How likely are you to do what the page asks you to do?
Scenario 3 (Q7_3) Malware Risk level: high	Get the latest WhatsApp stickers, click the following link: https://stickers.whatsapp.free.	How likely are you to do what the page asks you to do?
Scenario 4 (Q7_4) Clickjacking Risk level: medium	Two months free Netxxx premium subscription get free Netfxxx premium subscription anywhere in the world for 60 days. Get it now at https://bit[.]ly/3bDmzUw.	How likely are you to do what the page asks you to do?
Scenario 5 (Q7_5) Phishing Risk level: low	I am very sorry (to bother you with this message), dear sister. I am Indoxxxxx cashier staff, who needs a moment of your time. We had a customer who bought a game voucher, but entered the wrong cellphone number; thus, the SMS was sent to your number. Please check whether there is an SMS from WhatsApp with Thai writing on it and a 6-digit code for the fishing go game voucher. Help us to screenshot the SMS.	How likely are you to do what the page asks you to do?
Scenario 6 (Q7_6) Phising Risk level: low	Good afternoon, I am a representative from PT Makmur XXX. I want to place an order for goods from your company. Please send an offer letter to our company by attaching a complete ID card and identity. (remarks: this chat is sent from a WhatsApp business version account.)	How likely are you to do what the page asks you to do?

technical, and physical [23]. A social-based attack involves a scenario in which the attacker tries to persuade an individual target through psychological and emotional manipulation [17]. This is deemed to be more dangerous since humans naturally tend to trust one another compared to computers, making them a soft target for this approach. Another main classification of SECA is direct and indirect attacks. A direct attack is conducted via an interaction between attacker and victim, while an indirect attack is conducted via malware software, email, or messaging services [23].

The stages of SECA start from information gathering, followed by trust building, exploitation, and execution. Similarly, Salahdine and Kaabouch [23] identify the stages as research information collection, relationship development, exploitation, and execution and exit. In preparation of the action, the attackers build a relationship of trust with the victim [11]. The information gathered is then used for specific purposes or trade in the black market of data [23]. Breda et al. [22] further differentiated a SECA path attack according to the access that the attackers gain in order to exploit human vulnerabilities. Initially, this is through a social approach, with which the attackers use methods such as tailgating, impersonating, eavesdropping, shoulder surfing, and reverse social engineering, whereas the sociotechnical approach uses techniques such as phishing, baiting, and watering hole. The current study adopted the latter approach, with the three most commonly used techniques, phishing, baiting through malware, and clickjacking.

Phishing is the act of requesting detailed personal information such as the user's personal information, email, credit card details, pin, or password and then using this sensitive information to attack [10]. The lifecycle of a phishing attack includes the phase of planning and setup, the phishing attack itself, break in, data collection, and break out [24].

Clickjacking is an action designed to attract the victim with a shocking post or an essential document that is displayed as a PDF with the mouse pointer placed on the link and the actual URL in the status bar indicating that the document is a file that has to be clicked. This type of attack takes advantage of a victim's sense of curiosity using a video click as bait [14]. Once the victim clicks the video or image or post, the control of their computer is taken over by the attacker to acquire sensitive information or files.

Malware attack offers an application that allows users to achieve certain things, for example, to call and message their friends for free, if they give the application permission to access their profile and contact information and ignore the security warning message. Yan et al. [25] investigated malware propagation and found that malware can spread easily and exponentially in social network applications, thus becoming a serious threat in the system.

2.1.2. Behavioral Perspective of SECA: Habitual, Perception, and Socioemotional. Studies have argued that a person can be a victim of social engineering due to human weakness related to social-psychological factors [26]. These factors are the reason humans act in certain ways and can be affected by personality types, demographic variables, and motivations and drives.

The conceptual model of this study was based on three perspectives. The first is the habitual perspective, which measures the susceptibility of society to social engineering through the level of involvement, number of connections, and social network experience. Second is the perception perspective, which includes risk perception, competence, and cybercrime experience. The third is the social-emotional perspective, which consists of trust and motivation.

Habitual perspective is taken from the consumer behavior area, which refers to consumer decisions that are driven by habit, that is, decisions that are taken without much deliberation and comparison, other than what is considered repeating the same purchase out of habit. A related concept is consumer involvement, whereas low involvement might result in habitual behavior. In this study, the involvement of respondents in their social network is taken into account for social engineering susceptibility. It is hypothesized that higher involvement, connections, and experience contribute to higher susceptibility to a cyber attack (H_1).

Perception is defined as a person's understanding of the world around them [27]. The study of Alqarni et al. [28] on a social-media user's perception of a stranger's invitation found that the basis of accepting an invitation from a stranger is the perception risk arising from assessing their credibility. The perception of risk comprised the measure of severity should the event occur and the probability or likelihood of a cyberattack occurring. Furthermore, De Lange et al. [29] stated that a decision based on perception is strongly facilitated by experience. Thus, the evaluation of risk, competence, and previous experience formed a perception perspective based on the first hypothesis in this research. The hypotheses (H_2, H_3, and H_4) therefore suggested that perception perspective variables have a positive and significant relationship with susceptibility of SECA.

Along with habitual and perception perspectives, social and emotional state of being was believed to contribute to susceptibility of cyber attack. Previous studies found that motivation and trust in engaging with social media might contribute to one's susceptibility to cyberattack. Motivation is one of important factors to be investigated to predict certain behavior and therefore would provide insight into controlling SECA. Albladi and Weir's [18] expert's opinion suggested that one's motivation in engaging with a social network with low preventive measures can lead to cyber attack.

A study of consumer behavior defines motivation as utilitarian and hedonic [30, 31]. In the same light, Algarni et al. [26] categorized motivation of SECA into two types: need based and emotion-based behavior. Hedonic motivation results from the sensations one feels when engaging in social media messaging, while utilitarian motivation is derived from the function or "need" state of using the social media messaging application. Due to this typology, the motivation variable is hyphotize to comprise of hedonic and utilitarian motivation significantly contribute to the susceptibility of SECA (H_5).

Moreover, trust in technology is also identified as important variable which might contribute to one's susceptibility to cyber attack. The study of Pyke et al. [32] showed that propensity to trust is linked to the severity of cyber attacks. The current study aimed at differentiating between trust to the provider of technology (in this case, a social media provider) and trust to the member of the network (H_6 and H_7).

3. Results

The survey gathered 114 respondents through an online questionnaire and processed the responses for further analysis. The respondents' gender was 44.74% male and 55.26% women. Most respondents were young adults, aged 20-25 years (41.23%). The most recent education of the respondents was high school graduate (61.40%) followed by bachelor's (25.44%). The majority of respondents were in the group with monthly expenses of <USD 100, at 38.60%, followed by USD 100-200, at 28.07%, which is categorized as middle and lower-middle income class in Indonesia, which is the largest socioeconomic group. The current study conducted tests on whether demographic factors (age, gender, education, SES, and job position) influence susceptibility. The results show that all demographic variables have no influence on susceptibility since all results found were not significant.

3.1. Outer Model Analysis. The outer model result was tested against the criteria for reliability and validity. Cronbach's alpha was used as a measure of reliability. All variables had a Cronbach's alpha of more than 0.5 (>0.5), which suggests that the variables are reliable in measuring the construct. Composite reliability was tested as a measure of internal consistency with criteria larger than 0.7 (>0.7). The results show that all variables have a high internal consistency. Average variance extracted (AVE) was used to assess convergent validity. The value should be at least 0.5 (>0.5). Rounded values of all variables were shown to meet the criteria. The loading value of indicators should be larger than 0.5 (>0.5). The results omitted indicators that fell below 0.5 and retained a total of 37 indicators that met the criteria. Table 2 shows the mean and standard deviation of each

Table 2: Descriptive statistic and reliability test.

Variable	Indicators	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)
Competence					0.576	0.744	0.618
	Q8_8 < - competence	0.995	0.836	0.312			
	Q8_9 < - competence	0.497	0.506	0.351			
Cyber attack experience					0.834	0.889	0.668
	Q11_1 < - cyber attack experience	0.782	0.781	0.055			
	Q11_2 < - cyber attack experience	0.834	0.833	0.044			
	Q11_3 < - cyber attack experience	0.841	0.832	0.054			
	Q11_4 < - cyber attack experience	0.81	0.801	0.059			
Habitual perspective					0.529	0.728	0.481
	Q4 < - habitual perspective	0.856	0.79	0.209			
	Q5 < - habitual perspective	0.65	0.573	0.283			
	Q6 < - habitual perspective	0.534	0.457	0.304			
Likelihood_					0.802	0.884	0.717
	Q8_1 < - Likelihood_	0.884	0.884	0.028			
	Q8_2 < - Likelihood_	0.781	0.781	0.048			
	Q8_3 < - Likelihood_	0.871	0.871	0.029			
Motivation_					0.702	0.832	0.624
	Q10_1 < - Motivation_	0.777	0.749	0.14			
	Q10_2 < - Motivation_	0.752	0.733	0.114			
	Q10_4 < - Motivation_	0.838	0.832	0.084			
Risk perception					0.86	0.896	0.59
	Q8_2 < - risk perception	0.661	0.662	0.068			
	Q8_3 < - risk perception	0.786	0.786	0.045			
	Q8_4 < - risk perception	0.787	0.786	0.045			
	Q8_5 < - risk perception	0.846	0.847	0.033			
	Q8_6 < - risk perception	0.756	0.755	0.075			
Susceptability					0.879	0.908	0.623
	Q7_1 < - Susceptability	0.783	0.785	0.068			
	Q7_2 < - Susceptability	0.838	0.829	0.041			
	Q7_3 < - Susceptability	0.784	0.788	0.054			
	Q7_4 < - Susceptability	0.861	0.862	0.033			
	Q7_5 < - Susceptability	0.811	0.807	0.048			
	Q7_6 < - Susceptability	0.64	0.644	0.09			

Table 2: Continued.

Variable	Indicators	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)
Severity					0.869	0.92	0.793
	Q8_4 < - Severety	0.91	0.91	0.017			
	Q8_5 < - Severety	0.908	0.911	0.024			
	Q8_6 < - Severety	0.852	0.851	0.038			
Trust					0.903	0.926	0.675
Trust member					0.865	0.917	0.788
	Q9_1 < - trust member	0.878	0.874	0.036			
	Q9_2 < - trust member	0.917	0.913	0.035			
	Q9_3 < - trust member	0.867	0.867	0.043			
Trust provider					0.88	0.926	0.807
	Q9_4 < - trust provider	0.868	0.869	0.039			
	Q9_5 < - trust provider	0.92	0.921	0.017			
	Q9_6 < - trust provider	0.906	0.906	0.024			

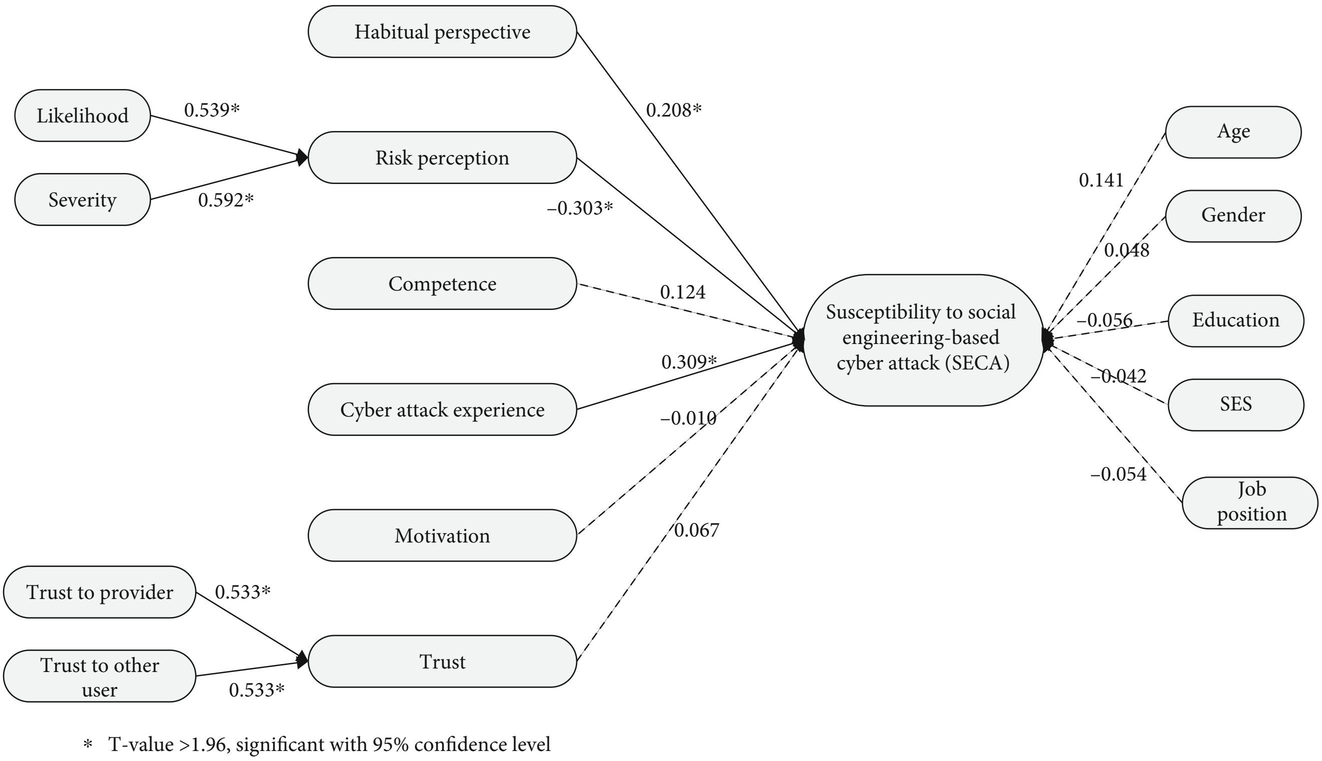

Figure 1: Inner model: loading values.

indicator. It can be concluded that the listed indicators were reliable and valid, and thus were ready to be further processed and analyzed for the inner (structural) model.

3.2. Inner Model. The inner model aims at testing the relationship between the latent variables as hypothesized. The bootstrapping process determines the significance of each relationship (T value), and the coefficient value measures the correlation between each variable. From the results (Figure 1), the variables that indicate a significant and positive relationship with susceptibility are habitual perspective, risk perception, and cyber attack experience. On the other hand, competence, motivation, and trust have been found not to significantly affect susceptibility. These findings are elaborated further in Section 3.3.

3.3. Discussion

3.3.1. Susceptibility. Susceptibility scenarios have become the main measurement of susceptibility to cyber attack based on social engineering. In this study, there were six scenarios developed based on a scale of 1 to 5, where 1 means never and 5 means definitely would carry out the instructions requested in the scenario developed.

As seen in Table 3, the results showed that 56.2% of respondents indicated that they were aware that the situation given in the scenario was suspicious and could lead to a method of attack via the chat messaging app; therefore, they chose not to fulfill the task requested in the scenario. However, the rest of the answers varied, which implies that some respondents are still susceptible to an attack. Moreover, the most susceptible scenario of selecting answers 4 and 5 (combined) is high. It was found that vulnerabilities were displayed when the respondent answered scenario 3, which offered WhatsApp stickers, followed by scenario 4, which invited users to download Netflix premium, and scenario 6, about a company's offer.

Further analysis shows that all scenarios were valid and reliable indicators of the susceptibility variable. The higher the value of the answers, the more susceptible the person is to social engineering-based cyberattack. In the next section, the relationship between the three perspectives and susceptibility is discussed to provide more insight into the driving factor of this construct.

3.3.2. Demographic Profile. The study found that the demographic variables were not validated as an indicator of one's susceptibility in this sample set. This finding contradicts Darwish et al., who found that demographic factors such as age, gender, education, and personality affect one's susceptibility to phishing attacks [33]. However, Gratian et al. [34] found no correlation between age and the user's effort for device securement, thus supporting the current research.

3.3.3. Habitual Perspective. The findings of this study show that habitual perspective has a significant and positive influence on susceptibility. This result implies that when the habitual perspective increases, one's susceptibility to SECA also increases, in the context of using a social media messaging application. This study is in accordance with research conducted by Albladi and Weir [18] and Molodetska et al. [35], which found frequent status updates and a high

Table 3: Susceptibility scenarios: result.

		% respondent answers for each scenario 1: never; 5: definitely.				
No	Option	1	2	3	4	5
1	Scenario 1 (Q7_1)	53.51%	22.81%	18.42%	4.39%	0.88%
2	Scenario 2 (Q7_2)	69.30%	10.53%	14.91%	4.39%	0.88%
3	Scenario 3 (Q7_3)	42.98%	16.67%	19.30%	15.79%	5.26%
4	Scenario 4 (Q7_4)	52.63%	18.42%	16.67%	9.65%	2.63%
5	Scenario 5 (Q7_5)	66.67%	14.91%	12.28%	5.26%	0.88%
6	Scenario 6 (Q7_6)	52.63%	19.30%	14.04%	10.53%	3.51%
Average		56.29%	17.11%	15.94%	8.34%	2.34%

number of contacts that comprise a habitual perspective can increase the level of susceptibility to SECA. Another study that indirectly supports this finding is by Darwish et al. [33], who found that a higher frequency of online shopping also leads to greater susceptibility to phishing attacks.

3.3.4. Perception Perspective: Risk Perception, Competence, and Cyberattack Experience. Perception perspective consists of risk perception, competence, and cyberattack experience. The study found that risk perception has a significant and negative influence on susceptibility. This indicates that when risk perception of a situation increases, the SECA decreases. Increasing one's perception of risk increases a person's ability to detect cyber threats or attacks, in other words, promoting precautionary behavior, which in turn makes a person less susceptible to cyber attacks [15, 18, 36].

Another driver of SECA susceptibility is cyberattack experience. The current result confirmed that experience has significant and positive effects on susceptibility to social engineering-based cyber attack. This implies that the more extensive the experience of cyberattacks, the more susceptible one is to cyber attack. It seems that when a person is targeted for a cyberattack, they have characteristics that increase their susceptibility to SECA.

Interestingly, competence was not found to have a significant effect on susceptibility. A previous study by Broadhurst et al. [37] explained that information technology (IT) competence did not greatly affect susceptibility. The participants who took part in the IT study indicated that IT competence would be significant, but most had no effect on security perceptions of susceptibility. A possible explanation, in this case, where cyber attacks use social engineering methods, is that some people carry out their actions by manipulation; thus, greater knowledge of IT has no relation to whether a person can be manipulated or not.

3.3.5. Socioemotional Perspective: Motivation and Trust. The results show that the susceptibility to social engineering-based cyberattacks is not caused by motivation or trust in the context of the current study. The motivation of someone to engage in social media messaging applications has not proven to be a determinant of their susceptibility to SECA. It implies that whether the motivation for engaging in social media messaging is hedonic, or utilitarian does not affect the likelihood of a cyberattack based on social engineering. In this context, it will be interesting to further elaborate whether low self-control is a better predictor of sustainability than motivation, as in the study of Nodeland [38]. In addition, the level of trust in the application provider or in a fellow user of social media messaging will not have an effect on SECA susceptibility. Although trust in online services is a factor to be considered by the users [39], it was not proved in the current study to be a determinant of one's SECA susceptibility.

4. Conclusions

The study's objective was to determine whether one's characteristics or behavior can be an identifying factor or a driving factor of susceptibility to social engineering-based cyberattack in the context of social media messaging services. The results of the current study imply that no demographic characteristic has an influence on susceptibility. Thus, a person's age, gender, education level, job position, and socioeconomic status might not indicate anything about the possibility of the person being more or less susceptible to SECA.

On the other hand, the study found three driving factors of susceptibility to SECA. The first is habitual: the habit of updating one's WhatsApp status and the number of contacts one has can increase one's susceptibility to SECA. The second is the perception of risk, the realization of severity, and the likelihood of the risk becoming an attack which can reduce susceptibility to SECA. The third is the experience of attack: as the occurrence and variability increase, it can also mean that a person is more susceptible to SECA. Interestingly, the study found that competence in IT is not a guarantee that a person is less susceptible to SECA, nor motivation and trust.

The results highlighted the important implications of increasing literacy in relation to cyber security. Siddiqi et al. [40] suggested methods to counter SECA and concluded that training and educating individuals about cybersecurity measures and SECA is the top priority. With greater knowledge of the risk of attacks, a person can be more alert to SECAs. This will be the responsibility of not only the government but also private institutions which provide services/products through the Internet. Consumers should be educated constantly about the risks of communicating via the Internet to increase their awareness. Secondly, cyber security policy regarding SECA needs to be designed, implemented, and communicated to entire organizations. There are ten aspects involved in the policies taxonomy, including access control policy and privacy policy [41].

The current study is not without limitations. Future studies could increase the sample size and the variety of user characteristics. Other types of social media providers could also be investigated to complement social media messaging. Further research could aim to identify other behavioral drivers of one's susceptibility to SECA, such as social influence, personality, or self-control.

Data Availability

The survey data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no potential conflict of interest.

Acknowledgments

The authors would like to acknowledge the generous research grant provided by Indonesia Banking School to conduct this study.

References

[1] International Labour Organization, *Working from home: estimating the worldwide potential*, ILO Policy Brief, 2020, October 2022, https://www.ilo.org/wcmsp5/groups/public/—ed_protect/—protrav/—travail/documents/briefingnote/wcms_743447.pdf.

[2] S. Venkatesha, K. R. Reddy, and B. R. Chandavarkar, "Social engineering attacks during the COVID-19 pandemic," *SN Computer Science*, vol. 2, no. 2, pp. 1–9, 2021.

[3] Deloitte, *Impact of Covid-19 on Cybersecurity*, Deloitte, 2022, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.htm.

[4] European Parliament, *Cybersecurity: main and emerging threats in 2021 (infographic)*, European Parliament, 2022, https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_en.pdf.

[5] B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," *Internet Technology Letters*, vol. 4, no. 2, article e247, 2021.

[6] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems*, vol. 67, no. 2, pp. 247–267, 2018.

[7] Purplesec, *Cyber-Security Trends in 2021*, Purplesec, 2021, https://purplesec.us/resources/cyber-security-statistics/.

[8] IBM, *X-Force Threat Intelligence Index 2022*, IBM, 2022, https://www.ibm.com/downloads/cas/ADLMYLAZ.

[9] Paloalto, *The State of Cybersecurity in ASEAN 2020*, Paloalto Networks, 2020, https://www.paloaltonetworks.sg/resources/whitepapers/the-state-of-cybersecurity-in-asean-2020.

[10] A. Sadiq, M. Anwar, R. A. Butt et al., "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0," *Human Behavior and Emerging Technologies*, vol. 3, no. 5, pp. 854–864, 2021.

[11] H. Aldawood and G. Skinner, "An advanced taxonomy for social engineering attacks," *International Journal of Computer Applications*, vol. 177, no. 30, pp. 1–11, 2020.

[12] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, 2003.

[13] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015.

[14] N. Duarte, N. Coelho, and T. Guarda, "Social engineering: the art of attacks," in *Advanced Research in Technologies, Information, Innovation and Sustainability*, pp. 474–483, Springer, Cham, 2021.

[15] P. Van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Computers in Human Behavior*, vol. 75, pp. 547–559, 2017.

[16] 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.

[17] C. Schroeder, *Susceptibility to Social Engineering: Human Vulnerabilities, [Ph.D. thesis]*, Utica College, 2019.

[18] S. M. Albladi and G. R. Weir, "Predicting individuals' vulnerability to social engineering in social networks," *Cybersecurity*, vol. 3, no. 1, pp. 1–19, 2020.

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

[20] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an ontological model defining the social engineering domain," in *ICT and Society. HCC 2014. IFIP Advances in Information and Communication Technology*, vol. 431, Springer, 2014.

[21] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of a social botnet," *Computer Networks*, vol. 57, no. 2, pp. 556–578, 2013.

[22] F. Breda, H. Barbosa, and T. Morais, "Social engineering and cyber security," in *11th International Technology, Education and Development Conference*, Valencia, Spain, 2017.

[23] F. Salahdine and N. Kaabouch, "Social engineering attacks: a survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019.

[24] B. B. G. Aakanksha, T. Ankit, K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3629–3654, 2017.

[25] G. Yan, G. Chen, S. Eidenbenz, and N. Li, "Malware propagation in online social networks," in *Proceedings of the 6th ACM symposium on information, computer and communications security-ASIACCS'11*, Hong Kong China, 2011.

[26] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: affect-based model," in *2013 IEEE Third International Conference on Information Science and Technology (ICIST)*, Yangzhou, China, 2013.

[27] R. Efron, "What Is Perception?," in *Proceedings of the Boston Colloquium for the Philosophy of Science 1966/1968*, pp. 137–173, Springer, Dordrecht, 1969.

[28] Z. Alqarni, A. Algarni, and Y. Xu, "Toward predicting susceptibility to phishing victimization on Facebook," in *2016 IEEE*

International Conference on Services Computing (SCC), pp. 419–426, San Francisco, CA, USA, 2016.

[29] F. P. De Lange, M. Heilbron, and P. Kok, "How do expectations shape perception?," *Trends in Cognitive Sciences*, vol. 22, no. 9, pp. 764–779, 2018.

[30] R. Batra and O. T. Ahtola, "Measuring the hedonic and utilitarian sources of consumer attitudes," *Marketing Letters*, vol. 2, no. 2, pp. 159–170, 1991.

[31] K. E. Voss, E. R. Spangenberg, and B. Grohmann, "Measuring the hedonic and utilitarian dimensions of consumer attitude," *Journal of Marketing Research*, vol. 40, no. 3, pp. 310–320, 2003.

[32] A. Pyke, E. Rovira, S. Murray, J. Pritts, C. L. Carp, and R. Thomson, "Predicting individual differences to cyber attacks: knowledge, arousal, emotional and trust responses," *Cyberpsychology*, vol. 15, no. 4, 2021.

[33] A. Darwish, A. E. Zarka, and F. Aloul, "Towards understanding phishing victims' profile," in *2012 International Conference on Computer Systems and Industrial Informatics*, pp. 1–5, 2012.

[34] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Security*, vol. 73, pp. 345–358, 2018.

[35] K. Molodetska, V. Solonnikov, O. Voitko, I. Humeniuk, O. Matsko, and O. Samchyshyn, "Counteraction to information influence in social networking services by means of fuzzy logic system," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 3, p. 2490, 2021.

[36] T. Nam, "Understanding the gap between perceived threats to and preparedness for cybersecurity," *Technology in Society*, vol. 58, article 101122, 2019.

[37] R. Broadhurst, K. Skinner, N. Sifniotis, B. Matamoros-Macias, and Y. Ipsen, "Phishing and Cybercrime Risks in a University Student Community," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 2, no. 1, pp. 4–23, 2019.

[38] B. Nodeland, "The effects of self-control on the cyber victim-offender overlap," *The International Journal of Cybersecurity Intelligence and Cybercrime*, vol. 3, no. 2, pp. 4–24, 2020.

[39] C. Iuga, J. R. C. Nurse, and A. Erola, "Baiting the hook: factors impacting susceptibility to phishing attacks," *Human-centric Computing and Information Sciences*, vol. 6, no. 1, 2016.

[40] M. A. Siddiqi, W. Pak, and M. A. Siddiqi, "A study on the psychology of social engineering-based cyberattacks and existing countermeasures," *Applied Sciences*, vol. 12, no. 12, p. 6042, 2022.

[41] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity enterprises policies: a comparative study," *Sensors*, vol. 22, no. 2, p. 538, 2022.