The Benefit of Warning to Improve Detecting Social Engineering Attack Messages

Ibrahim Mohammed Alseadoon

Department of Information and Computer Science, College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia
Email: i.alsedon@uoh.edu.sa (I.M.A.)

Manuscript received March 12, 2024; revised May 8, 2024; accepted June 12, 2024; published August 19, 2024

***Abstract*—Social engineering attack messages are a constant threat to online services. Numerous scholars have attempted to solve this problem by understanding the interaction between users and social engineering attack messages. Users' behavior and traits are crucial in making them immune to attacks. Specifically, studies have indicated that the mental process of detection has a tremendous effect on preventing users from becoming victims of attacks. Studies have also suggested that users need to think in a certain way to detect deception. Our study aims to determine the impact of warnings on users' types of thinking to increase secure behavior. A mixed-method approach is applied (i.e. experiment and open-ended questions) to answer research questions. The results indicate that warnings impact users' types of thinking and have a significant impact on increasing their protection against attacks. In addition, warnings have the benefit of confirming users' initial judgment of known (familiar) social engineering attack messages without the need to perform deep thinking to identify deception. Additionally, users employ several methods to validate messages. Warning has an effect on these methods.**

***Keywords*—cybersecurity, information security, social engineering, detection**

I. Introduction

Social engineering attacks cause enormous losses for individuals and organizations [1, 2]. Studies have tackled the issue of social engineering attacks by improving users' detection capability [3]. Raising awareness and providing training to tackle social engineering attacks are the main methods for handling users' weaknesses [4]. Furthermore, various researchers have paid a great deal of attention to methods such as updating software and being cautious on the internet. Technical solutions have not yet been able to provide total protection, even with the application of artificial intelligence techniques [5]. Therefore, users should always be included in the defence mechanism.

Improving users' awareness increases their defence against social engineering attacks [6–9]. Specifically, several studies have reported that understanding users' thinking techniques while encountering deceptive messages can help improve their ability to detect attacks [10, 11]. In this context, users have two main routes of thinking: (1) the central route and (2) the peripheral route [12]. Studies claim that the central route is more effective at making users better detectors. Additionally, the theory of deception indicates that users can detect deception by observing the differences between what is shown and what is expected in a message [13–15]. Most education programs have evolved around improving users' expectations of legitimate and illegitimate messages. Expectation serves as a baseline for detection. To elaborate, any message behaving differently from the baseline should be suspected.

Although many studies encourage taking a central route for detection, the current study claims that users can detect social engineering attacks effectively by taking the peripheral route. For example, users can identify and avoid familiar social engineering attack messages as soon as they encounter them. Users do not need to apply new techniques or conduct further investigations when they detect a known deceptive message. Therefore, the peripheral route also protects users from known social engineering attack messages. In contrast, the central route is crucial in protecting users from new and advanced deceptive messages. Social engineering attack messages always apply new deceptive techniques to lure users.

An additional issue that the current study tries to resolve is that most users do not apply the detection mode while interacting with messages. Users judge messages based on previous experience. Prejudged messages from certain entities can make users less careful. Social engineering messages benefit from the trust organizations or individuals have gained to make users behave in a certain way (e.g. clicking on links). If users continue to use the peripheral route when encountering deceptive messages, they will eventually fall victim to attacks. What encourages users to continue to use the peripheral route is their sense of safety while surfing the internet. Users are under the impression that social engineering attacks will not target them or that they have nothing to lose. This kind of mental thinking makes users less willing to be cautious in applying the central route or to behave securely.

Another danger facing internet users is a lack of experience or, in other words, a baseline to compare messages with. Inexperienced users and new services are introduced daily. Particularly after the COVID-19 pandemic, many organizations began offering online services. Many employees worked from home, and many students studied online. This enormous shift created a conducive environment for attackers. More users became available online, especially naïve users who had just been introduced to online services and were unfamiliar with them. This unfamiliar environment encouraged users to accept and adopt new ways of communication with which they were unfamiliar. These types of users are a danger to the safety of organizations. Naïve users do not have enough experience (i.e. a baseline) to differentiate between legitimate and illegitimate messages.

Understanding how to effectively improve users' types of thinking while they interact with social engineering messages is critical. Several studies suggest that encouraging users to implement the central route when making decisions is

important [10, 11]. For example, it is normal for a user to communicate with friends on the internet. An attacker can compromise a user's online account. Then, the attacker can send messages requesting money from the compromised account to the user's contact list. In this case, if the recipient is not able to conduct deep thinking about the sender's abnormal behavior, they will become a victim of social engineering attack messages. Therefore, making users cautious (not paranoid) about the messages they receive is important for protecting them on the internet. To achieve this goal, users should be encouraged to change their usual type of thinking to apply the central route.

The current study attempts to understand what motivates users to apply the central route. Directly asking users to always apply the central route while interacting with messages may cause them to lose interest in detection and to behave carelessly. The central route requires much thinking. Users need to apply various methods to validate their hypotheses (i.e. their judgement). Therefore, users should be incentivized to apply the central route without causing them to lose interest in detection. Furthermore, users need to be supported with on-the-spot tools to improve and validate their decisions. For example, a user may receive a message from a friend or organization requesting that they behave abnormally. The user may suspect the request, but they will still need other methods to verify whether the message is legitimate [16]. Therefore, organizations should be encouraged to support their employees and customers with ways to confirm or deny suspicious messages.

II. Literature Review

Defences against social engineering attack messages started being developed from the moment these attacks were discovered. The focus was on technical solutions because they are the most accredited and powerful defences against such attacks (from the perspective of experts). However, technical solutions cannot prevent all attacks. Some attacks manage to reach users, who are the final line of defence. Users' defences can be improved in different ways, as explained below.

According to the literature, attempts to improve users' ability to detect social engineering attack messages focus on two main aspects: (1) awareness and (2) training [4]. Many studies target the awareness aspect to tackle the problem of social engineering attacks from the perspective of less knowledgeable or less experienced users. A study found that even information technology (IT) staff members, who are expected to be experienced, often need to take awareness programs to increase their defences against attacks [17]. Users' carelessness also contributes to this problem. Users may know about the existence and danger of social engineering attacks. However, they may still not take the necessary steps to protect themselves or their organisations. For example, some users choose weak passwords, some are not cautious on the internet, some do not behave securely on the internet, and some rely solely on software or on the organisation's systems to protect them from danger. Such carelessness merits more attention from researchers.

Many studies have shown that educating users about social engineering attacks, such as phishing, makes them more immune against these types of attacks [6, 8, 9]. Informing users on how to identify social engineering messages improves their detection capabilities. Furthermore, users can gain detection capabilities through work experience or by interacting with their peers. However, the problem with training is improving users' ability to detect certain attacks. Because attackers are constantly developing new attack methods, users will always be vulnerable to zero-day attacks. Attackers always have the advantage of knowing, based on experience, which technique will be successful and which will not. Organizations and users may be surprised by attacks they are not ready to manage and have no defences against.

Users' characteristics and backgrounds are also responsible for affecting their detection behavior [18–20]. Users' traits such as openness, agreeableness, extraversion, and submissiveness have been found to influence their susceptibility to attacks. Although users' traits are difficult to change with training and education, their vulnerability can be reduced.

Perceived danger is another factor affecting users' behavior regarding attack messages. Junger *et al*. found that users were more willing to disclose private information when monetary incentives were introduced [21]. Perceived danger can change users' behavior from that of a risk taker to that of a risk-averse individual. Risk-taker users tend to respond to deceptive messages if they do not perceive any danger in doing so [18]. This tendency can be reduced when they perceive more danger in responding than in ignoring messages. Perceived danger in responding to messages has the effect of making risk-taker users recall all their perceived knowledge and experience to make reliable judgements. In the end, such users avoid responding to social engineering attack messages.

One key factor that has not received enough research in the realm of social engineering attacks is warning [3]. The current study attempts to fill this gap by identifying the impact of warnings on users' types of thinking.

III. Methodology and Model

Our study adopted two types of research methodologies: experiment and qualitative (i.e. role-play and open-ended research questions). The participants were randomly divided into two groups (see Fig. 1). The first group was the controlled group, in which participants were asked to rate their responses to messages (whether to click or not to click) on a 5-point Likert scale [22]. The second group was the informed group. The participants were informed that some messages in the experiment were social engineering attack messages, but they were not given any hints about those messages or taught any detection techniques. The experiment started with the controlled group first and the informed group second to avoid any leakage of information about the nature of the experiment and to avoid giving time to the participants to prepare or train themselves to become better detectors.

The first experiment had 34 participants, and the second experiment had 28 participants. In both groups, the participants were shown five messages. These messages were a mix of legitimate messages and social engineering attack messages. The participants had to use their abilities and skills to identify the latter. They were not taught any detection

techniques or given any prior cybersecurity education. Two questions were asked: (1) Explain the reasons behind your decision to click on the message link and (2) explain the reasons behind your decision not to click on the message link. The participants' answers were recorded using Google Forms [23]. These questions were asked to answer the current study's hypotheses, which are listed below.

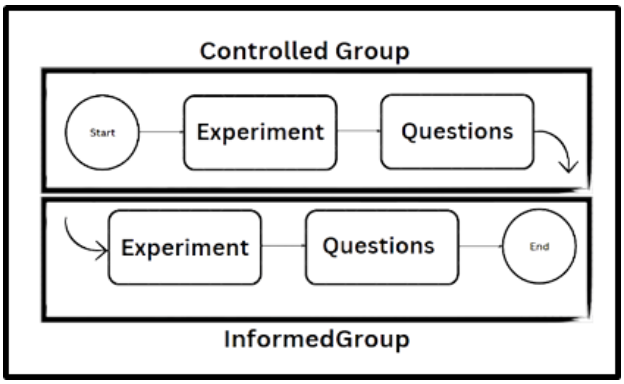

Fig. 1. Research methodology.

A. Hypotheses

H1: The central route type of thinking can be triggered by warning users about the potential danger of receiving social engineering attack messages.

In the literature, scholars have proposed that the central route is key for the detection of attack messages [11]. The current study suggests that the central route can be triggered by warning users about the potential danger of receiving such messages. Users can shift their thinking to the central route if the idea of an attack is fresh in their minds. When users think a message is a hoax, they apply their knowledge and skills to their decisions.

H2: The peripheral route type of thinking can be used to identify known social engineering attack messages and legitimate messages.

Although the focus of the literature has shifted to the central route, the peripheral route can also help identify messages. Specifically, it can help in identifying (1) familiar attack messages that use a certain attack technique (e.g. offering to send enormous sums of money) and (2) legitimate messages from known entities.

H3: The central route type of thinking can be used to identify unknown social engineering attack messages and abnormal behavior in messages from known entities.

New types of messages and behaviors need to be judged using the central route, which can help in identifying (1) unfamiliar attack messages from unknown entities and (2) abnormal behavior in messages from known entities.

IV. The Peripheral Route type of Thinking

The peripheral route can help users identify known social engineering attack messages and legitimate messages from known entities. Users may be familiar with certain types of attack messages. These messages do not require users to shift their type of thinking to the central route to recognize them or to perform further validation and make reliable decisions. Users can rely on their initial decision not to respond to deceptive messages and to trust legitimate messages.

A. Known Attack Messages

Awareness and education programs have taught users to recognize certain types of social engineering attack messages. When they encounter these messages, they apply their sense of responsibility and make reliable decisions to avoid them. Alseadoon [24] found that users are cautious when interacting with known social engineering attack messages. Additionally, awareness and education programs have improved users' detection abilities and granted them lasting knowledge.

B. Known Messages from Known Entities

Users normally receive messages from their friends and familiar organizations. When receiving such messages, users can interact with them safely and without immediate danger. This is particularly true when a request in these messages is a common request.

Known messages can shape the baseline for users for the kinds of messages they expect from known entities, whether the entity is a person or an organization. Unfamiliar messages (new types of messages), which can be social engineering attack messages, can pose a threat when users have not developed a baseline to determine whether the messages are legitimate.

V. The Central Route type of Thinking

The central route can help users identify unknown attack messages (i.e. new messages) and abnormal behavior in known entity messages.

A. Unknown Attacks

Users perceive these kinds of messages as new because of the nature of the messages or the requests in the messages. For example, a new organization may ask users to send certain types of information or act in a certain way. In this situation, users need guidance to make reliable decisions. Users may choose to ignore these messages, but the consequences of doing so may not be clear. These messages require users to perform deep thinking and analysis before responding. Researchers should pay more attention to these messages because they are vital in preventing users from becoming victims of attack messages.

B. Abnormal Messages from Known Entities

Users are familiar with the kinds of messages they normally receive from friends or organizations. However, they may receive an abnormal request from these friends or organizations. For example, if a friend's account is compromised, the attacker may try to communicate with that friend's contacts and ask them to send money. This abnormal behavior may attract users' attention. However, because the attacker may frame the situation as urgent and use emotional language, users may fall victim to the attack. Additionally, organizations are always informing their employees and clients that they will never request the latter's password. Nevertheless, some employees and clients in certain situations tend to reveal their passwords.

Verification of abnormal behavior in messages can reduce the probability of successful deception. Verification can be achieved by using different methods of confirmation. The

identification of deceptive messages can only occur when users suspect a message and have prior knowledge that social media accounts can be compromised. Organizations can reduce deception by introducing certain types of verification behaviors. Furthermore, organizations need to encourage users to report any abnormal behavior in messages. Users may sometimes be in a dilemma about engaging in certain types of behaviors. For example, it is normal for employees to receive messages from their superiors about performing certain types of tasks. However, even if an employee suspects that a message is fake, they may consider it unprofessional to verify it with their superiors. Organizations need to employ a reliable channel to make verification easier and more achievable for employees. Attackers always rely on weak channels of communication among employees in organizations. Attackers also try to impersonate trustworthy entities to increase their opportunities to achieve a successful attack.

VI. Results and Discussion

Our study implemented thematic analysis and found that there are four main methods that participants use to judge a message, as supported by the literature. The results supported that warnings have impacted three main methods and shifted users' decision-making to become more resilient in their judgments.

A. Appearance

The participants used appearance to judge a message. The first impression that users have while interacting with messages is vital. A message that is perceived as professional will have more legitimacy. Participants judged a message's appearance based on certain words, message time, logo design, and Uniform Resource Locator (URL) design. Appearance judgment is done by the peripheral route.

Our study found that reliance on appearance was slightly reduced in the second experiment. In the first experiment, 34 percent of the participants relied on a message's appearance to make a judgment. Meanwhile, in the second experiment, 28 percent of the participants relied on a message's appearance to make a judgment. Participants searched for deep signs to judge a message.

B. Trust

Trust is another strategy that participants use to judge a message. Some participants did not clearly explain what cues made them lose trust in certain messages (e.g. a feeling that the message was untrustworthy). However, trust is not the strongest strategy for participants to make judgements. For example, some participants stated that the entity behind a message should be trustworthy. The danger behind this thinking is that attackers can apply it to lure users into revealing sensitive information. Some participants trusted the legitimacy of a message based on their perceptions alone.

Our study found that trust behavior significantly shifted between the two experiments. In the first experiment, the participants placed high reliance on trust to judge messages; 45 percent of the participants used the trust technique. However, in the second experiment, the percentage dropped dramatically; only 28 percent of the participants used this technique even after they were informed about the nature of the study. It can be said that participants apply deep thinking strategies to evaluate messages. The participants went from giving trust by only seeing certain cues in a message (peripheral route) to searching for inconsistency between the cues shown in a message and their real meaning technically (central route). For example, one participant stated that when he receives messages asking him to act in a certain way, he evaluates that request by logging into his account and checking whether the request is legitimate. He said that he never clicks on email links directly.

C. Sender (Source)

One of the criteria that the participants applied to judging messages was to examine the sender. If the sender was a known entity, the participants chose to click on the message link. Some participants stated that messages from government or well-known organizations were legitimate. This kind of thinking is dangerous because social engineering attacks repeatedly impersonate known entities to lure users into taking certain actions that benefit attackers.

Our study found no difference in participant behavior between the two experiments. Twenty-eight percent of the participants in both experiments used sender information to judge the messages' authenticity. It can be said that the participants, as they were in their early stages of computer studies, did not accumulate enough knowledge to gain technical ways of evaluating message sources (as normal users are).

D. URL

Surprisingly, most participants in the second experiment showed a high interest in examining URLs for legitimacy. Even though some of their methods were incorrect, the participants closely examined URLs after being warned about social engineering attack messages. For example, some participants stated that seeing Hypertext Transfer Protocol Secure (HTTPS) in URLs is a high indication of safety. HTTPS indicates that the connection is encrypted. It is true that the participants had some security knowledge. However, it was not strong enough to make reliable judgments. The participants needed to know more about the different techniques for evaluating messages.

Our study found significant differences among the participants' behaviors in the two experiments. In the first experiment, around 48 percent of the participants relied on URLs to authenticate messages, whereas in the second experiment, 68 percent of the participants relied on URLs to authenticate messages. Unfortunately, some participants' evaluation methods were ineffective. It can be said that evaluating URLs requires deep thinking to come to a decision on whether a link is legitimate. It depends heavily on which participants significantly shifted to central thinking.

VII. Discussion

It was found in the current study that different users, when warned about social engineering attacks, tended to behave differently. Users become more alert, increase their secure behaviors, and behave more responsibly. Additionally, the current study found that users become more risk-averse after

receiving such a warning.

Even if users already have knowledge about social engineering attacks, this knowledge may not help them identify social engineering attack messages. Users' detection abilities need to be improved to make them immune to such attacks. For example, some users examine links in messages; however, their judgements may not be correct. The existence of 'https' and 'gov' in URLs gives a sense of legitimacy. However, these elements can be misleading.

The crucial finding of our study is that when warned about social engineering messages, users shifted their thinking from the peripheral route to the central route. This kind of thinking strategy is encouraged to increase users' chances of successful detection. Users are triggered to authenticate messages and become less likely to interact with suspected messages. This kind of behavior is encouraged in organizations. Additionally, to strengthen an organization's protection, users should also be encouraged to report suspicious messages; however, this behavior needs further investigation [25].

There are four main criteria for judging messages: (1) Message appearance and a sense of professionalism – these criteria play a vital role in creating legitimacy. Appearance is the first step in detection. According to the model of detection [11], users are always judging messages based on what they have experienced. Any mismatch between expectations and reality triggers users' suspicion. (2) Trust – Trust fades away when users are warned about attack messages. Users depend less on trust and try various tangible ways to validate messages. (3) Source of a message – Users are highly dependent on this to judge a message. However, users need more education on this criterion because they can be tricked. (4) URLs – Users are highly reliant on URLs to authenticate messages. However, users need more information and techniques to make robust judgements based on URLs.

There are two main recommendations for organizations. The first recommendation is that users should be informed about the potential risks of social engineering attacks. Users should be able to use this knowledge to make reliable judgements. Providing information about behaving securely on the internet and about attack techniques can keep users triggered. One drawback of this method is the possibility of employees not responding to work messages, which affects workflow and delays some projects and tasks.

The second recommendation is to provide a supporting team from the IT department. Users sometimes do not come to a clear-cut decision about whether a message is legitimate. Some messages can be ambiguous. In this case, the IT team can step in. The benefit of this step is that it leads to higher education about internet security. Studies have shown that learning on the spot is an effective method [26]. In other words, when users suspect a message and receive assistance from the IT department, this experience will remain with them for a long time.

Finally, in the literature on social engineering, there is a heavy emphasis on users implementing a central route to increase users' protection against attacks. Our study found that the peripheral route can also be as beneficial in detection as the central route. The peripheral route helps users detect and identify known social engineering attack messages; users should trust their judgement and act accordingly. There is no need to take more time or conduct further investigations.

VIII. Conclusion

Our study tried to fill the gap in the knowledge about how warnings affect users' intellectual processes when encountered with social engineering attack messages. The study presented the participants with two types of messages: legitimate messages and social engineering attack messages. The participants were randomly divided into two groups: one group was not warned about social engineering messages, and the other group was informed that some messages were social engineering messages without identifying them. The participants were not given any hints, training or any detection tools. The results supported the hypotheses and proved that warnings can shift users' types of thinking to the central route for unknown messages. Additionally, users changed their behavior and became more vigilant about social engineering attack messages. Furthermore, the results showed that well-known social engineering attack messages do not require users to perform any kind of validation. Users can easily identify them using only the peripheral route and avoid further investigation.

In summary, warnings shifted users' behavior according to four main criteria that they applied to judge messages. However, some of these criteria need more refinement to enable users to make robust judgements. Additionally, users occasionally need external support to validate their judgements. In this case, organizations are encouraged to provide users with proper support.

One of the limitations in our study is that the participants were warned about social engineering attacks during the experiment (only warning, no training or facilitating cybersecurity tools), which may not happen in the real world. However, the study was designed to determine the impact of warnings on users' behaviors. Therefore, it was necessary to provide warnings during the experiment. Future research can distinguish between giving warnings and studying behavior with messages. Organizations can still benefit from our study results by continually educating and warning their users about deceptive messages.

Conflict of Interest

The author declares no conflict of interest.

References

[1] C. Nightingale, *Social Engineering Insights 2020*, 2020.

[2] F.B.I. *Internet Crime Complaint Center Releases 2022 Statistics*. (2023). [Online]. Available: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

[3] S. Baki and R. Verma, "Sixteen years of phishing user studies: What have we learned?" *IEEE Transactions on Dependable Secure Computing*, vol. 14, no. 8, pp. 1–13, 2022.

[4] M. Guilford, *Systemic Risk Analysis of Human Factors in Phishing*, Old Dominion University, 2023, p. 127.

[5] P. J. Uppalapati *et al*., "A machine learning approach to identifying phishing websites: A comparative study of classification models and ensemble learning techniques," *EAI Endorsed Transactions on Scalable Information Systems*, Online First Articles, no. 1, p. 9, 2023.

[6] F. Alotaibi *et al*., "Design and evaluation of mobile games for enhancing cyber security awareness," J*ournal of Internet Technology and Secured Transactions*, vol. 6, no. 2, pp. 569–578, 2018.

[7] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Computers & Security*, vol. 73, pp. 519–544, 2018.
[8] P. Kumaraguru *et al*., "School of phish: a real-world evaluation of anti-phishing training," in *Proc. the 5th Symposium on Usable Privacy and Security*, Mountain View, California, USA: Association for Computing Machinery, 2009.
[9] S. Sheng *et al*., "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish," in *Proc. the 3rd symposium on Usable Privacy and Security*, Pittsburgh, Pennsylvania, USA: Association for Computing Machinery, 2007.
[10] S. Grazioli, "Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet," *Group Decision Negotiation*, vol. 13, pp. 149–172, 2004.
[11] R. Wright *et al*., "Where did they go right? Understanding the deception in phishing communications," *Group Decision and Negotiation*, vol. 19, no. 4, pp. 391–416, 2010.
[12] R. E. Petty and J. T. Cacioppo, *The Elaboration Likelihood Model of Persuasion*, Academic Press, 1986, pp. 123–205.
[13] P. E. Johnson *et al*., "Detecting deception: adversarial problem solving in a low base-rate world," *Cognitive Science*, vol. 25, no. 3, pp. 355–392, 2001.
[14] P. E. Johnson, S. Grazioli, and K. Jamal, "Fraud detection: Intentionality and deception in cognition," *Accounting, Organizations and Society*, vol. 18, no. 5, pp. 467–488, 1993.
[15] P. E. Johnson *et al*., "Success and failure in expert reasoning," *Organizational Behavior and Human Decision Processes*, vol. 53, no. 2, pp. 173–203, 1992.
[16] I. M. Alseadoon *et al*., "Typology of phishing email victims based on their behavioural response," in *Proc. the Nineteenth Americas Conference on Information Systems (AMCIS 2013)*, Chicago, Illinois, USA: Association for Information Systems (AIS), 2013.
[17] S. Benqdara, "Building an information security awareness program for a private financial organization: Case from Libya," *International Journal of Computer Applications*, vol. 185, no. 1, pp. 28–34, 2023.
[18] I. M. A. Alseadoon, *The Impact of Users' Characteristics on Their Ability to Detect Phishing Emails*, 2014, QUT: Brisbane, Australia.
[19] I. Alseadoon, M. Othman, and T. Chan, "What is the influence of users' characteristics on their ability to detect phishing emails?" in *Advanced Computer and Communication Engineering Technology*, A.S. Hamzah, et al., Eds. Switzerland: Springer, 2015, pp. 949–962.
[20] M. K. Tornblad *et al*., *Characteristics that Predict Phishing Susceptibility: A Review*, vol. 65, no. 1, pp. 938–942, 2021.
[21] M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Computers in Human Behavior*, vol. 66, pp. 75–87, 2017.
[22] R. Likert, "A technique for the measurement of attitudes," *Archives of Psychology*, vol. 22, no. 140, p. 55, 1932.
[23] Google. *Google Forms: Online Form Creator | Google Workspace*. (2023). [Online]. Available: https://www.google.com/forms/about/
[24] I. M. Alseadoon, "The power of intention in detecting social engineering attacks," *International Journal on Information Technologies and Security*, vol. 15, no. 3, pp. 75–86, 2023.
[25] I. A. Marin *et al*., "*The influence of human factors on the intention to report phishing emails*," in *Proc. the 2023 CHI Conference on Human Factors in Computing Systems*, 2023.
[26] R. A. Schmidt and R. A. Bjork, "New conceptualizations of practice: Common principles in three paradigms suggest new concepts for training," *Psychological Science*, vol. 3, vol. 4: pp. 207–218, 1992.