Factors Influencing Players’ Susceptibility to Social Engineering in Social Gaming Networks

AHMAD ALTURKI1, NORA ALSHWIHI1, AND ABDULLAH ALGARNI2

1Department of Information Systems, Faculty of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
2Information Technology Division, Institute of Public Administration, Riyadh 11141, Saudi Arabia

Corresponding author: Nora Alshwihi (nalshwihi@gmail.com)

The authors would like to thank Deanship of Scientific Research (DSR), in King Saud University, for funding and supporting this research through the initiative of DSR Graduate Students Research Support (GSR).

ABSTRACT Social gaming networks have become a new phenomenon, especially for young people, who may become addicted to some extent. However, this phenomenon also increases their susceptibility to hacking, cyber-attack, and other types of security breaches. Various studies have found that current technology is inadequate in terms of online security. Thus, researchers have started to pay attention to the human aspect of security, which is based on interactions with strangers who may trick other gamers into revealing personal or financial information, that is, social engineering. There is little in the social gaming network literature to help players, researchers, and organizations to address the human aspect of online security, and thus there is a need to investigate the factors affecting this aspect of security. The current study aims to identify the factors influencing social engineering victimization in social gaming networks. The model developed in this study is based on the health belief model and cooperation and competition theory. The results show that the perceived severity of the threat, perceived barriers, perceived benefits, self-efficacy, competition, and cooperation are significant factors in the prediction of social engineering victimization.

INDEX TERMS Social engineering, social gaming networks, competition, cooperation, susceptibility, health belief model.

I. INTRODUCTION

Social games enable people to enjoy interacting with both friends and strangers, and online gaming has created significant social networks over the last decade. A 2015 US survey found that 72% of teenagers played games, 75% of them online, and of those, 54% only played with friends online, while 52% also played with strangers online [1].

Social gaming networks (SGNs) are defined as computer networks that are simultaneously inhabited by multiple players for the purpose of playing games. As SGNs are Internet-based and offer people the opportunity to interact with others and exchange information, they significantly increase people’s susceptibility to various types of threats. Greenhill [2] found that 55% of players had experienced, either directly or indirectly, some form of victimization while playing games online.

Security threats in relation to online gaming include two types: human threats, which are based on interactions with strangers who may trick others into revealing personal or financial information (so-called social engineering); and technology-based threats, which are based on computer programs including viruses, Trojan horses, worms, and spyware [3].

The most significant security threats are posed by social engineering [4]–[7], which is “a term used to describe how one person persuades another person to access confidential information or to give them the information that they want” [6]. However, although the term itself is brief and straightforward, social engineering is clever and complex in nature. There are some circumstances in which victims have little time to think, such as instances of attention blindness or situations where their anger or stress enable social engineers to exploit them using tactics designed to obtain their trust, such as pretending to help the victim so that they can obtain the desired information [4].

Social engineering in SGNs is a serious problem in terms of information security, and developers and designers of software applications are continually working to address this issue. However, at present there is little to help players, researchers, and organizations in addressing the problem because the underlying factors have not yet been thoroughly
investigated. Most studies on SGNs have focused on security and cyber-attacks related to software architecture, violent content, virtual property, cheating, and modifying game software or networks [8]–[10]. Because technology alone is insufficient to ensure the security of players, researchers have realized that it is necessary to consider the human aspect of security [11]. Identifying and understanding the human factors that lead players to fall victim to social engineering will support awareness raising and training programs for players and society in general, and the optimization of detection software to provide advanced solutions, as well as enabling future studies to identify better solutions and mitigate social engineering attacks in SGNs.

In this study, we aim to identify the factors influencing players’ behavior in response to social engineering victimization and to identify the relationships among cooperation, competition, and social engineering victimization.

The rest of the paper is organized as follows. Section 2 presents a review of the relevant literature, Section 3 discusses the theoretical background and presents several hypotheses, Section 4 explains the methodology, Section 5 tests the hypotheses and reviews the results, and Section 6 concludes with a discussion of the results and a summary of the contributions and limitations of this study.

II. LITERATURE REVIEW

Several studies have investigated social engineering in social networks. For example, Algarni identified various types of social engineering attacks on social networking sites, along with the objectives of those attacks and the reasons why various individuals fell victim to such attacks. The results showed that the main tool used in social engineering is impersonation [12]. Albladi also examined the factors causing users to be more susceptible to social engineering attacks including their online habits, personality traits, and demographics [13]. Another study found that users who are highly active on social networking sites are more susceptible to attack than less-active users [14]. A study investigating how social networking habits can influence users’ vulnerability to attacks found that victimization through social engineering can be predicted based on the degree of social media usage, which has a significant influence on the likelihood of an individual being attacked [15].

Although some researchers have studied social engineering in relation to social networks, social gaming environments involve different behaviors and methods of social engineering attacks than general social networking sites, leaving players even more vulnerable to social engineering attacks. For example, in a game-playing situation involving cooperation, research suggests that players fail to adequately check about 95% of the emails they receive, trusting them implicitly if they appear to have been sent by a friend [16]. Moreover, Waddell and Peng found that players do not appear to differentiate between friends and strangers with regard to in-game collaboration [17]. Several studies [18]–[20] have found that cooperative game-playing situations lead players to erroneously help, share information with, or trust other people more than they would do otherwise. Furthermore, studies have found that a player’s reputation can significantly improve the level of cooperation they receive. Influential players are more able to persuade other players [21], [22]. Thus, other players’ susceptibility to social engineering victimization increases [6], [23].

Most social networking sites provide their services for free (e.g., Twitter, Facebook, and Snapchat). However, most SGNs charge players a fee to download or play a game. Furthermore, the prices of some of the games are relatively high. In 2010, the Pew Research Center found that 65% of Internet users had paid money to download or access digital content, while only 19% had paid for online games [24]. This has created the temptation for players to think about stealing money from other players’ accounts so that they can purchase and play new games. In addition, it may cause potential players who cannot afford the price of a game to fall victim to phishing attacks when they try to access games from fake websites that are offering the games for free.

Most online gaming sites have online stores, and players’ gaming accounts are usually connected to their payment information. Once an attacker obtains access to a player’s account, the attacker can obtain the player’s credit card information and even make use of any account balance (or games that have been paid for). Attacks have also occurred in relation to trading of games when there has been no security mechanism in place to protect players. Players often like to exchange games, but some players have not had their games returned. It was reported that one person earned around US$11,000 through this type of behavior by accepting money from players but not sending any games [9]. This results in both a financial impact and a psychological impact on players who have behaved honestly.

This study focuses on players’ behavior in response to social engineering attacks, with the aim of increasing players’ knowledge and security while using SGNs. We attempt to predict players’ susceptibility to falling victim to a social engineering attack in an SGN based on behavioral factors and to identify the relationships among competition, cooperation, and susceptibility to social engineering attacks.

III. THEORETICAL BACKGROUND AND HYPOTHESES

A. HEALTH BELIEF MODEL (HBM)

Numerous studies have applied theories from the healthcare domain to the investigation of information security [25]–[27]. “The health belief model (HBM) is a model that attempts to predict and explain behavioral intentions or the likelihood of an individual’s behavior” [28]. The HBM contains four core constructs. The first is dependent on two beliefs regarding threats, namely, the perceived severity of threats and perceived susceptibility to threats. The second involves evaluating behavior, which is dependent on the perceived benefits of preventing threats through specific behaviors and the perceived cost of the preventive behavior. The third construct, which is a recent addition, involves cues to action. Cues to
action include a diverse range of triggers such as security education and advice from others. The fourth construct is self-efficacy, which is defined as a user's confidence in his or her ability to undertake a specific behavior [28], [29].

Studies on security-related behavior investigating the perceived severity of and susceptibility to threats have produced inconsistent findings. Workman found that people's perceptions of the severity of the threat and their susceptibility to threats affected their responses to a social engineering threat [23], while other studies have found that perceived susceptibility to a threat has a significant impact on behavior, although the perceived severity of the threat does not [25], [30], [31]. Conversely, Tsai found that the perceived severity of a threat was a significant predictor of behavior intended to enhance online safety, while perceived susceptibility to a threat was not [32]. Despite these contradictory findings, the general consensus among researchers is that both perceived susceptibility to threats and the perceived severity of threats have a positive impact on behavior designed to increase players' security. Therefore, in this study, we assume that at least one of these factors influences players' behavior in response to the possibility of social engineering attacks. Thus, the following hypotheses are proposed in relation to the abovementioned constructs:

**H1:** the perceived severity of a threat in an SGN is negatively correlated with social engineering victimization.

**H2:** the perceived susceptibility to a threat in an SGN is negatively correlated with social engineering victimization.

Perceived barriers are a significant factor in reducing behavior aimed at mitigating threats to players' security [30], [31]. These include the perceptions that exercising security measures while playing the game is time-consuming and that anti-phishing software will affect performance. Therefore, there is a high probability of a social engineering attack in an SGN environment. Thus, we propose the following hypothesis:

**H3:** the level of perceived barriers to online games-related security is positively correlated with social engineering victimization.

The perceived benefit construct used in this study aims to determine to what degree a player agrees to exercise security-related behavior to protect them from social engineering threats. Thus, we propose the following hypothesis:

**H4:** the perceived benefit of online games-related security behavior is negatively correlated with social engineering victimization.

Most previous studies have found that individuals with a high level of self-efficacy are extremely cautious about making online payments, and thus make very few payments. These studies have concluded that self-efficacy is a vital element in mitigating risky online behavior [25], [26], [33], [34]. In this study, we expect that a player with a high level of self-efficacy is likely to follow the recommended security-related behaviors while playing online games and respond positively to the necessary security measures. Therefore, we propose the following hypothesis:

**H5:** self-efficacy in SGNs is negatively correlated with social engineering victimization.

In the HBM, cues to action can include both external triggers such as knowledge of other individuals experiencing security issues, security awareness programs, and media alerts regarding security vulnerabilities, and internal triggers such as previous experience of the problems that can occur [26], [35]. While cues to action may be important, to date there have been few studies focusing on this topic [30]. However, Dodel found that previous experiences are directly linked to preventive behaviors [35]. Thus, in this study, we aim to determine whether cues to action affect players' responses to social engineering attempts. Thus, we propose the following hypothesis:

**H6:** Cues to action in SGNs are negatively correlated with social engineering victimization.

**B. COMPETITION AND COOPERATION THEORY**

A key element in understanding the nature of cooperation and competition is the type of goal interdependence that is identified among players. Goals may exhibit negative interdependence, that is, one player’s success may correlate with the other’s failure. Such situations tend to involve competitive relationships with a win–lose orientation. Alternatively, goals may exhibit positive interdependence, where the success of one player is correlated with the success of another, while failure of one is correlated with failure of the other. These situations tend to involve cooperative relationships with a win–win orientation [8], [36].

Cooperation is induced by perceived similarities in relation to beliefs and attitudes, a willingness to be helpful, openness in communication, and a trusting, friendly attitude [36], [37]. Thus, it can be seen that there is a positive correlation between cooperation and susceptibility to social engineering victimization. Numerous studies such as [18]–[20] have found that trust is the key to cooperation, whereas other studies have found that trust is a key factor in social engineering success [4], [23]. Thus, it is expected that some players will respond to deceptive behaviors. Therefore, we propose the following hypothesis:

**H7:** Cooperation in SGNs is positively correlated with social engineering victimization.

The opposite effect can be seen in relation to competitive situations because it is difficult to maintain trust in communications between competitors [38]. Previous studies have found that competition is associated with very little information, as it almost completely eliminates the element of trust [39], [40]. Thus, we propose the following hypothesis:

**H8:** Competition in SGNs is negatively correlated with social engineering victimization.

**IV. METHOD**

**A. SCALE DEVELOPMENT AND TESTING**

A quantitative approach was used to test the eight hypotheses. This is the most frequently used approach in the field of
information systems [41]. Pre-test items relating to the HBM and competition and cooperation theory were developed to address the research items and guide the survey question design. Pre-existing scales were used in most of the scenarios. The scales developed in earlier studies have been verified for reliability and validity, although we tested them again prior to our analysis.

To extract a better measure, the strategy recommended by Churchill and Dedic has been followed [42]. The first step in their strategy involves specifying the construct domain. In this study, we reviewed the literature in relevant disciplines such as health, information technology, psychology, sociology, behaviorism, and human communication to discover any potentially essential constructs. It was found that the concepts of the HBM and competition and cooperation theory have been conceptualized and operationalized for various purposes using different samples and populations in fields other than our area of interest. The second step involves refinement of the item sample, whereby a sample of items is chosen from the initial pool. The challenges at this point are related to adjusting these concepts to fit the background and context of information security and social engineering attacks while retaining item validity.

The Delphi method was used to test and develop the items while reducing the error factor and make the questions more specific to SGNs. The items are shown in Table 1. A five-point Likert scale was used to measure responses to all of the items and SPSS version 25.0 statistical software was used to analyze the data.

### B. PILOT STUDY

A pilot study was conducted to test the measurement scale before undertaking the main study. The purpose of the pilot study was to validate the measurement scale for every factor related to social engineering in SGNs. The experimental design and procedures for the pilot study were similar to those of the main study, although the participant selection strategy differed. The participants in the pilot study were selected based on convenience and their willingness and ability to participate. Thirty participants completed the survey, of which 60% were male and 40% were female. All of the participants in the pilot study were from Saudi Arabia. Analysis of the data from the pilot study showed that in terms of reliability, Cronbach’s alpha was 0.79, as shown in Figure 1.

### C. APPROACH AND SAMPLE

In the online gaming environment, most gamers are members of social networks and know each other, especially the famous players. Thus, the snowballing method is the best approach. The online survey was distributed through these groups via their accounts on various social networking sites (e.g., Instagram, WhatsApp, Twitter, and Facebook). In the Twitter application, we asked famous Saudi gamers to support the study by completing the survey and then retweeting it to other players’ accounts. We also sent the survey directly to players’ private statements with the request that they distribute it to other players. We received 302 responses, all from Saudi Arabia.

### V. DATA SCREENING AND FACTOR ANALYSIS

We commenced our analysis by addressing all of the requirements of structural equation modeling (SEM) including limited missing values, freedom from extreme outliers, lack of significant distortion by specific groups, and assumptions of normality and linearity. Then, we computed the reliability of the scales using Cronbach’s alpha.

As shown in Table 2, factor analysis revealed nine factors with an eigenvalue of 1 or greater and the minimum Cronbach’s alpha value was 0.70. The overall Kaiser–Meyer–Olkin measure of sampling adequacy was 0.76 ($P < 0.0001$), and the total variance was 1.2. The overall reliability of the items used in the survey based on Cronbach’s alpha was 0.72.

### VI. TESTING THE HYPOTHESES

The hypotheses proposed the existence of negative correlations between social engineering victimization and the perceived severity of the threat, perceived susceptibility to threats, perceived benefits, cues to action, self-efficacy, and competition, while they proposed a positive correlation between susceptibility to social engineering victimization and perceived barriers and cooperation.

To improve validity and provide further explanation of the impacts of the various factors involved in the hypotheses, multiple regression analyses were undertaken using SPSS. The model included a dependent variable, namely, social engineering victimization, and eight independent variables, namely, perceived severity, perceived susceptibility, perceived barriers, perceived benefits, cues to action, self-efficacy, competition, and cooperation.

In addition, it was important to examine how well the model was fitted using plot diagrams. Figure 2 shows that the data were normally distributed, while the scatter plot in Figure 3 shows that there was a high linear correlation and
TABLE 1. Survey items.

| Construct                  | Sample item after refinement                                                                 | Ref |
|----------------------------|-----------------------------------------------------------------------------------------------|-----|
| Cooperation                | I enjoy playing with others to achieve a joint win. To win, one must cooperate with others.     | [43]|
|                            | I like to cooperate with other gamers. I can learn important things from other gamers.         | [19]|
| Competition                | It is important to me that I do better than others. I enjoy the challenge of competing against others to win. | [43]|
|                            | I like the challenge of seeing who is the best. I don’t like to come second.                   | [19]|
| Perceived severity of a threat | The potential trouble caused by social engineering affects me while I am using social gaming networks. It would be a very serious problem if I became a victim of social engineering while using social gaming networks. I get depressed when I think about social engineering attacks while using social gaming networks. | [44]|
|                            | I am afraid to even think about social engineering while using social gaming networks.         | [29]|
| Perceived susceptibility to threats | It is extremely likely that my information will be infected by a social engineering attack on social gaming networks. | [44]|
|                            | There is a good possibility that I will be subjected to a social engineering attack while using social gaming networks. | [45]|
|                            | My chance of being subjected to a social engineering attack while using social gaming networks is high. | [44]|
|                            | I feel that I could be vulnerable to a social engineering attack through social gaming networks. | [46]|
| Perceived barriers         | Exercising care would change the way I use my computer.                                        | [31]|
|                            | Use of specific software for security costs time and effort.                                   | [31]|
|                            | Exercising care when playing games on social gaming networks makes me uncomfortable. Exercising care when playing games on social gaming networks is inconvenient. | [29]|
| Perceived benefits         | Having social engineering awareness when using social gaming networks protects me from attack. Using security software is a good investment to reduce my vulnerability to a social engineering attack. Being cautious before helping other gamers on social gaming networks helps prevent a social engineering attack. | [48]|
|                            | [47]                                                                                           |
| Cues to action             | If a gamer started behaving strangely and asked me for personal information, I would be concerned that I might be a victim of a social engineering attack. If one of my friends experienced a social engineering attack, I would be more cautious about making payments and giving out my information. If I saw a new report or read about a new vulnerability to social engineering attacks, I would be more concerned about my chance of being attacked. If I received an email from the game store provider about a new security protocol, I would feel more cautious about playing the game. | [31]|
| Self-efficacy              | I can select appropriate gamers for my social gaming network.                                   | [31]|
|                            | In general, I am safe from social engineering threats. I have the knowledge to secure myself against a social engineering attack. Taking the necessary security to prevent social engineering attacks while using social gaming networks is easy. | [49]|

The coefficients are presented in Table 3. It can be seen that perceived barriers was the strongest predictor ($\beta = 0.540$, $p < 0.0001$), followed by perceived severity of threats ($\beta = -0.208$, $p < 0.0001$), competition ($\beta = -0.146$, $p < 0.01$), self-efficacy ($\beta = -0.136$, $p <0.01$), cooperation ($\beta = 0.135$, $p < 0.01$), and perceived benefits ($\beta = -0.122$, $p < 0.01$). Neither perceived susceptibility nor cues to action were significant predictors of social engineering victimization ($p > 0.05$).

The results displayed good variance as shown in Table 4 ($R = 0.708$, $R^2 = 0.501$). The residual value was good (minimum $= -2.50$, maximum $= 1.75$), Cook’s distance was 0.1, tolerance was less than 1, and VIF was less than 10.

VII. STRUCTURAL MODEL FIT ASSESSMENT

SEM is a multistep technique that is used to assess the validity of a theoretical model by evaluating the relationships between the constructs in such a model, while taking into account measurement errors during statistical analysis [50]. SEM is considered to be an extension of multivariate statistical methods such as regression analysis.

In this study, SEM involved two main tasks. The first task was addressing the data requirements, as explained in Section V, while the second task was examining the goodness close relationship between social engineering victimization and most factors (perceived severity of threats, perceived barriers, perceived benefits, self-efficacy, competition, and cooperation).
of fit of the model [51]. The model assessment process included examining the standardized path coefficients of the relationships included in the model and examining the model fit indices [50].

The results of the testing of the final model using SPSS AMOS are shown in Figure 4. All correlation coefficients were significant predictors of susceptibility to social engineering, supporting six of the hypotheses. Further assessment was undertaken regarding the goodness of fit. The model appears to display good fit, with the minimum discrepancy (chi-square, \( \chi^2 \)) divided by the degrees of freedom (df) < 5.0, the comparative fit index = 0.90, the incremental fit index = 0.902, and the root mean square error of approximation = 0.04. These values satisfy the requirements of SEM [50] and are presented in Table 5.

### VIII. DEMOGRAPHIC ANALYSIS

In this section, we examine the relationship between the players’ demographics and social engineering victimization by measuring players’ overall susceptibility to social engineering victimization. The results presented in Table 6 show...
that gender has a significant effect on susceptibility to social engineering victimization (p = 0.002), with ANOVA analysis showing that males are more susceptible to social engineering than females (mean for females = 3.33 and mean for males = 3.73).

IX. DISCUSSION AND CONCLUSION

● Summary of Results

In this study, we investigated the factors that are associated with susceptibility to social engineering victimization in SGNs. The components of the proposed model are derived from the HBM and competition and cooperation theory. Eight hypotheses were proposed and tested, and six were found to be supported.

The results showed a significant relationship between perceived severity of threats and social engineering victimization. Of the other factors, perceived barriers were the most significant predictor of social engineering victimization. Perceived benefits were also found to have an influence on responses to social engineering attacks.

There was a significantly negative relationship between self-efficacy and susceptibility to social engineering victimization, supporting the findings of most of the previous studies on online security behavior [25], [26], [29]. Our findings also indicate that both cooperation and competition have a significant relationship with social engineering victimization.

Conversely, perceived susceptibility and cues to action did not have a significant impact on susceptibility to social engineering victimization. Inconsistent findings and unexpected results are common in studies related to virtual environments such as SGNs, with one study finding that individual behavior on social networking sites differs from that displayed in real-world situations [52]. However, the unsupported hypotheses require further investigation, and present opportunities for future research.

● Contribution

In this study, we investigated the relationship between falling victim to social engineering attacks in a new environment such as SGNs, which exhibit different characteristics to other social networks. We applied two important theories (the HBM and cooperation and competition theory), which have been developed in different disciplines, to a crucial problem in relation to online information security, namely, social engineering in SGNs.

This study makes a significant contribution to the literature in several fields including information systems, information science, and cybersecurity. In terms of user susceptibility, several information systems studies have investigated individuals’ susceptibility to security victimization using various theories and techniques, such as protection motivation theory (e.g., [53]–[55]), electroencephalography (e.g., [56]), technology threat avoidance theory ([57]), and routine activity theory (e.g., [58]). This study contributes to this stream of research by identifying the impact of players’ susceptibility to social engineering victimization in a new environment, namely, SGNs.

In addition, this study makes a significant contribution by providing increased understanding of and a possible solution to a serious problem in the field of information security. Players have been found to be extremely vulnerable to falling victim to various social engineering threats including phishing, clickjacking, pretexting, financial abuse, and identity theft.

Furthermore, this study is unique in pinpointing the high level of threat presented by social engineering in SGNs. The findings of this study can be used in conjunction with the findings of previous studies to address social engineering victimization issues.

Automated tools have been established and promoted to alert users to potentially fraudulent websites and emails, but even though these tools are useful, social engineering continues to occur. Tools and software are not sufficient to protect people from online social engineering attacks. They can prevent frequent technical attacks, but not social engineering attacks. One study used 200 verified phishing URLs from two sources and 516 legitimate URLs to test the effectiveness of 10 popular anti-phishing tools and found that only one tool was able to consistently identify more than 90% of phishing URLs correctly. However, it also incorrectly identified 42% of legitimate URLs as phishing URLs. Of the remaining tools, only one correctly identified more than 60% of phishing URLs from both sources [59]. Moreover, another study found that 97% of the participants in our experiment were successfully deceived by at least one of the phishing messages that we sent them. When they issued a “passive warning,” only one participant heeded the warning [60]. The findings of our study will help to identify the best solution to the problem of social engineering attacks by identifying the factors affecting people’s susceptibility to these attacks.

The results of this study are important for organizational policy makers who aim to control insider threats based on theoretical knowledge. Many organisations allow their employees to use SGNs while at work. While it is important for organisations to utilise technical security defences, the result of this study shows that it is more important to utilise behavioural defences and improve employees’ capabilities to

### TABLE 5. Model fit statistics.

| Model Fit Indices for the Model Without Structural Relationships | \( \chi^2 \) (CMIN) | DF | \( \chi^2/DF \) | IFI | CFI | RMSEA |
|---|---|---|---|---|---|---|
| | 514.316 | 314 | 3.58 | 0.902 | 0.90 | 0.04 |

### TABLE 6. Summary of demographic results.

| Regression Analysis | Variance Tests | Mean | |
|---|---|---|---|
| Gender | Standardized Coefficient | Sig | F value | Sig | Females | Males |
| | | | | | 3.33 | 3.73 |
defend against such attacks. For example, the results of this study showed that enhancing employees’ perceived severity of social engineering threat, and perceived barriers, can help in improving employees’ capabilities to defend against social engineering. Enhancing employees’ perceived severity of social engineering threat, and perceived barriers can be done through raising employees’ awareness, which can be done using training, brochures, and others tools.

In addition, organisations are recommended to have a set of policies that control how employees use SGNs while at work, and they should consider the factors that have been highlighted in this study when making policies. Those factors have been found to be very influential on users’ decisions to accept or reject threats. Furthermore, auditing and testing have also been suggested as important countermeasures to address human vulnerabilities. Organisations are encouraged to use the factors that have been found in this study when testing their employees’ abilities to react to social engineering tricks.

The findings of this study have also a number of important implications for individuals, parents, educators, and SGNs providers. For example, individuals are advised to use the results of this study, especially the results of the competition and cooperation situations, in order to determine their special vulnerabilities. In addition, the results of this study indicate that it is useful for parents to enhance children’s perceived cost, in comparison to perceived benefit, when dealing with strangers in SGNs. The findings of this study will also be helpful in deriving a set of best practices such as SETA programs and computer monitoring, which have been identified the best way to avoid or mitigate human-based information security incidents [61]. Educators are encouraged to take the results of this study in considerations, and provide guidelines and specific educational curricula that address children and youth safety in SGNs. Finally, SGNs providers are encouraged to promote the usage of some online games to help show children how to make responsible decisions about online communication and learn about key issues of digital world. Online activities can include exploration of methods of communication in chat rooms, social gaming networks, and emails.

REFERENCES

[1] A. Lenhart. (2015). Teens, Technology and Friendships. Accessed: Jan. 3, 2018. [Online]. Available: http://www.pewinternet.org/2015/06/06/Teens-Technology-And-Friendships/  
[2] R. Greenhill. (1997). Diablo, and Online Multiplayer Game’s Future. Games Domain Review. [Online]. Available: http://www.gamesdomain.com/gdreview/depart/jun97/diablo.html  
[3] J. H. Stewart, Jr., “Social engineering deception susceptibility: Modification of personality traits susceptible to social engineering manipulation to acquire information through attack and exploitation.” Ph.D. dissertation, Colorado Tech. Univ., Colorado Springs, CO, USA, Jun. 2015, p. 92.  
[4] C. Hadnagy, Social Engineering: The Art Of Human Hacking, Hoboken, NJ, USA: Wiley, 2010.  
[5] J. Kee, “Social engineering: Manipulating the source,” GCIA Gold Certif., SAS Inst., Bethesda, MD, USA, Tech. Rep., Oct. 2008.  
[6] R. E. Indrajit, “Social engineering framework: Understanding the deception approach to human element of security,” Int. J. Comput. Sci. Issues, vol. 14, no. 2, pp. 8–16, 2017.

[7] M. Perc, M. Ozer, and H. Holnik, “Social and juristic challenges of artificial intelligence,” Palgrave Commun., vol. 5, no. 1, pp. 1–7, Dec. 2019.

[8] R. J. Robles, S.-S. Yeo, Y.-D. Moon, G. Park, and S. Kim, “Online games and security issues,” in Proc. 2nd Int. Conf. Future Gener. Commun. Netw., Dec. 2008, pp. 145–148.

[9] Hanksoreh. (2001). Online Cheating is Ubiquitous. Accessed: Mar. 9, 2001. Available: [Online]. Available: http://www.hanmi.co.kr/section005100025/2001/05/005100025200105091907004.html

[10] J. Ki, J. H. Cheon, J. Kang, and D. Kim, “Taxonomy of online game security,” Electron. Library, vol. 22, no. 1, pp. 65–73, Feb. 2004.

[11] F.-C. Chang, C.-H. Chiu, N.-F. Miao, P.-H. Chen, C.-M. Lee, T.-F. Huang, and Y.-C. Pan, “Online gaming and risks predict cyberbullying perpetration and victimization in adolescents,” Int. J. Public Health, vol. 60, no. 2, pp. 157–166, Feb. 2015.

[12] A. Algarni, Y. Xu, and T. Chan, “Social engineering in social networking sites: The art of impersonation,” in Proc. IEEE Int. Conf. Services Comput., Jun. 2014, pp. 797–804.

[13] S. Albladi and G. R. S. Weir, “Vulnerability to social engineering in social networking networks: A proposed user-centric framework,” in Proc. IEEE Int. Conf. Cybercrime Comput. Forensics (ICCCF), Jun. 2016, pp. 1–6.

[14] T. W. Amm, O. Okhrina, J. Lu, and J. A. Tang, “A comprehensive analysis of phishing on a social system,” Dep. Electr. Comput. Eng., Dec. 2010.

[15] A. Vishwanath, T. Herath, R. Ch, J. Wang, and H. R. Rao, “Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model,” Decis. Support Syst., vol. 51, no. 3, pp. 576–586, Jun. 2011.

[16] A. B. Wire. (2011). Phishing Game Consists Majority of Online Users Vulnerable to Attack. Accessed: Apr. 10, 2020. http://search.ebscohost.com.sdl.oid.ucoln.org/login.aspx?direct=true&db=rps&AN=bizwire.c31915178&site=eds-live

[17] J. C. Waddell and W. Peng, “Does it matter with whom you play? The effects of competition, cooperation and relationship type among video game players,” Comput. Hum. Behav., vol. 38, pp. 331–338, Sep. 2014.

[18] K. S. Cook, R. Hardin, and M. Levi, “Cooperation Without Trust,” New York, NY, USA: Russell Sage Foundation, 2005.

[19] R. J. Grisham, Student Attitudes Toward Competitive Cooperative and Individualistic Classroom Goal Structures. Wright-Patterson AFB, OH, USA: Air Force Inst Of Tech, 1991.

[20] T. Yamagishi, S. Kanazawa, R. Mashima, and S. Terai, “Separating trust from cooperation in a dynamic relationship: Prisoner’s dilemma with variable dependence,” Rationality Soc., vol. 17, no. 3, pp. 273–308, Aug. 2005.

[21] H.-H. Chen, L. Wang, S.-W. Sun, J. Wang, and C.-Y. Xia, “Evolution of cooperation in the spatial public goods game with adaptive reputation assortment,” Phys. Lett. A, vol. 380, nos. 1–2, pp. 40–47, Jan. 2016.

[22] C. Xia, S. Ding, C. Wang, J. Wang, and Z. Chen, “Risk analysis and enhancement of cooperation yielded by the individual reputation in the spatial public goods game,” IEEE Syst. J., vol. 11, no. 3, pp. 1516–1525, Sep. 2017.

[23] M. Workman, “A test of interventions for security threats from social engineering,” Inf. Manage. Comput. Secur., vol. 16, no. 5, pp. 463–483, Nov. 2008.

[24] J. Jansen. (2010). Internet Users Have Paid for Online Content. [Online]. Available: http://www.pewinternet.org/2010/12/30/65-Of-Internet-Users-Have-Paid-For-Online-Content/  
[25] B.-Y. Ng, A. Kankanhalli, and Y. Xu, “Studying users’ computer security behavior: A health belief perspective,” Decis. Support Syst., vol. 46, no. 4, pp. 815–825, Mar. 2008.

[26] C. Xia, “The adoption of computer security: An analysis of home personal computer user behavior using the health belief model,” Ph.D. dissertation, Manage. Inf. Syst. Commons, Utah State Univ., Logan, UT, USA, 2011, p. 149.

[27] N. Davidson and E. Silence, “It won’t happen to me: Promoting secure behaviour among Internet users,” Comput. Hum. Behav., vol. 26, no. 6, pp. 1739–1747, Nov. 2010.

[28] M. K. Janz and M. H. Becker, “The health belief model: A decade later,” Health Educ. Quart., vol. 11, no. 1, pp. 1–47, Mar. 1984.

[29] V. L. Champion, “Instrument development for health belief model constructs,” Adv. Nurs. Sci., vol. 6, pp. 73–85, 1984.

[30] C. J. Carpenter, “A meta-analysis of the effectiveness of health belief model variables in predicting behavior,” Health Commun., vol. 25, no. 8, pp. 661–669, Nov. 2010. [Online]. Available: https://doi.org/10.1080/10410236.2010.521906
[31] C. L. Ciar and J. Johnson, “Analyzing home PC security adoption behavior,” J. Comput. Inf. Syst, vol. 4, pp. 20–29, Dec. 2012.

[32] H.-Y.-S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifen, and S. R. Cotten, “Understanding online safety behaviors: A protection motivation theory perspective,” Comput. Secur., vol. 59, pp. 138–150, Jun. 2016.

[33] G. R. Milne, L. I. Labrecque, and C. Cromer, “Toward an understanding of the online Consumer’s risky behavior and protection practices,” J. Consum. Affairs, vol. 43, no. 3, pp. 449–473, Sep. 2009.

[34] H.-S. Rhee, C. Kim, and Y. U. Ryu, “Self-efficacy in information security: Its influence on end users’ information security practice behavior,” Comput. Secur., vol. 28, no. 8, pp. 816–826, Nov. 2009.

[35] M. Dodel and G. Mesch, “Cyber-victimization preventive behavior: A health belief model approach,” Comput. Hum. Behav., vol. 68, pp. 359–367, Mar. 2017.

[36] M. Deutsch, “Cooperation and competition,” in Conflict, Interdependence. Noida, Uttar Pradesh: Justice, 2011, pp. 23–40.

[37] D. Tjosvold and D. Johnson, “Deutsch’s theory of cooperation and competition,” in Work Teams: Past, Present and Future. Dordrecht, The Netherlands: Springer, 2000, pp. 131–155.

[38] D. W. Johnson and R. T. Johnson, Cooperation and Competition: Theory and Research. Edina, MN, USA: Interaction Book, 1989.

[39] S. Huck, G. K. Länsler, and J.-R. Tyran, “Competition fosters trust,” Games Econ. Behav., vol. 76, no. 1, pp. 195–209, Sep. 2012.

[40] G. Liu, C. Lin, and Z. Xin, “The effects of Within- and between-group competition on trust and trustworthiness among acquaintances,” PLoS ONE, vol. 9, no. 7, 2012, Art. no. e103074.

[41] J. Recker, Scientific Research in Information Systems: A Beginner’s Guide. Springer, 2012, pp. 1.2.2, 1.2.9.

[42] G. A. Churchill, “A paradigm for developing better measures of marketing constructs,” J. Marketing Res., vol. 16, no. 1, p. 64, Feb. 1979. [Online]. Available: www.jstor.org/stable/3150876. Accessed 20 Apr. 2020.

[43] C. H. Simmons, E. A. Wehner, S. S. Tucker, and C. S. King, “The cooperative/competitive strategy scale: A measure of motivation to use cooperative or competitive strategies for success,” J. Social Psychol., vol. 128, no. 2, 199.5, Apr. 1998.

[44] N. A. G. Arachchilage and S. Love, “A game design framework for avoiding phishing attacks,” Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714, May 2013.

[45] B.-Y. Ng, A. Kankanhalli, and X. Xu, “Studying users’ computer security behavior: A health belief perspective,” Decis. Support Syst., vol. 46, no. 4, pp. 819–825, Mar. 2009.

[46] M. Chan, I. Woon, and A. Kankanhalli, “Perceptions of information security in the workplace: Linking information security climate to compliant behavior,” J. Inf. Privacy Secur., vol. 1, no. 3, pp. 18–41, Jul. 2005.

[47] A. Soleymanian, S. Niknami, E. Hajizadeh, D. Shojaieizadeh, and A. Montazeri, “Development and validation of a health belief model-based instrument for measuring factors influencing exercise behaviors to prevent osteoporosis in pre-menopausal women (HOPE),” BMC Musculoskeletal Disorders, vol. 15, no. 1, p. 61, Apr. 2014.

[48] M. T. U. Soto, “Studying phishing attacks: An alternative approach to phishing,” J. Assoc. Inf. Syst., vol. 39, no. 1, pp. 1, 91–112, Jan. 2015.

[49] Z. Alqarni, A. Algarni, and Y. Xu, “Toward predicting susceptibility to social engineering in social gaming networks,” MIS Quart., vol. 39, no. 1, pp. 61–84, Jun. 2014.

[50] I. Woon and H. R. Rao, “Insider threats in a financial institution: Analysis of attack-proneness of information systems applications,” MIS Quart., vol. 39, no. 1, pp. 1, 91–112, Jan. 2015.

[51] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, “Phishing phish: Evaluating anti-phishing tools,” Tech. Rep., 2016.

[52] S. Egelman, L. F. Cranor, and J. Hong, “You’ve been warned: An empirical study of the effectiveness of Web browser phishing warnings,” in Proc. 26th Annu. CHI Conf. Hum. Factors Comput. Syst., 2008, pp. 1065–1074.

[53] J. D. Arcey, A. Hovav, and D. Galletta, “User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach,” Inf. Syst. Res., vol. 20, no. 1, pp. 79–98, Mar. 2009.

AHMAD ALTURKI was born in Riyadh, Saudi Arabia, in 1978. He received the B.S. degree in information systems from King Saud University, Saudi Arabia, in 2000, and the M.S. and Ph.D. degrees in information systems from the Queensland University of Technology, in 2009 and 2014, respectively. He is currently an Assistant Professor with the Department of Information Systems, King Saud University, a position he has held since 2014. He is the author of more than ten published articles. He is a Scientific Reviewer of two journals and two conferences. His research interests include business process management, entrepreneurship, design research in information systems, enterprise resource planning systems, and design science research methodology in information systems. He was a recipient of the Best Dissertation Award from the Australian 2014.

NORA ALSHWI was born in Riyadh, Saudi Arabia, in 1992. She received the B.S. degree from Imam Muhammad Ibn Saud Islamic University, in 2016, and the M.S. degree in information systems from King Saud University, in 2019. Her research interests include cybersecurity, social engineering, information behavior, and information security.

ABDULLAH ALGARNI received the B.S. degree in computer science from King Abdulaziz University, Saudi Arabia, the M.S. degree in computer science from Western Michigan University, USA, and the Ph.D. degree in computer science from the Queensland University of Technology, Australia. He is currently an Assistant Professor with the Division of Information Technology and the Director of Innovation and Business Development at the Institute of Public Administration, Saudi Arabia. His current research interests are mainly in the areas of social engineering, phishing, deception, and information security management. He has published several articles in journals, such as EJHS, IEEE ACCESS, and JEEE, and in international conferences, such as ICIS, HICSS, and PACIS by the Australian Council of Professors and Heads of Information Systems (ACPHIS), in 2014.

[54] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower, “Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders,” Inf. Manag., vol. 51, no. 5, pp. 551–567, 2014.

[55] A. Vance, B. Anderson, C. B. Kirwan, D. Eargle, and B. Young, “Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG),” J. Assoc. Inf. Syst., vol. 15, no. 10, pp. 679–722, 2014.