Personality Traits and Cyber-Attack Victimisation: Multiple Mediation Analysis

Samar Muslah Albladi and George R S Weir
Department of Computer and Information Sciences
University of Strathclyde
Glasgow, UK
{samar.albladi; george.weir}@strath.ac.uk

***Abstract*—The current research aims to gain insight on the role of the five personality traits (conscientiousness, neuroticism, extraversion, agreeableness, and openness to experience) in users' susceptibility to cyber-attack victimisation in the context of online social networks and investigates how different factors such as users' competence to deal with online threats, users' trust in other members in social network as well as trusting the network's service provider, users' motivation to engage in the network, and users' experience with cyber-crimes mediate and control this relationship. The effect of personality traits on user's online risky behaviour is still a controversial topic in cyber security research. Therefore, the present study proposes a mediation model that includes the five personality traits and the four mediators that together affect the user's likelihood of falling victim to cyber-attacks. The study conducted a scenario-based experiment with 316 participants to test the study model and the hypotheses' significance. Empirical results indicate that all five personality traits, except openness, have significant indirect effect on users' susceptibility to cyber-attack victimisation.**

Keywords— Cyber-attack, Motivation, Personality Traits, Trust, User Competence, User Vulnerability

I. INTRODUCTION

According to the big five personality traits theory [1], there are five distinct traits (conscientiousness, neuroticism, extraversion, agreeableness, and openness to experience) that explain the pattern of human personality in regard to their reactions, behaviours, feelings, and thoughts. This theory has been widely adopted and discussed by many researchers. Personality traits are commonly known as the driver of human behaviour and have been recognized by researchers from diverse fields, such as marketing [2] and entrepreneurship [3], as predictors of user reactions to different phenomena. Previous information security research has anticipated the relationship between the big five personality traits and the user's likely victimisation to cyber-attacks such as social engineering-based attacks. Some research has empirically investigated personality traits' impact on email phishing responses [4], [5]. However, Halevi et al. [4] state that neuroticism is the only trait that correlates to phishing email responses, while the Alseadoon et al. [5] study presented opposing findings that openness, extraversion, and agreeableness are personality traits that increase user tendency to comply with phishing email requests. One potential reason for such inconsistent results is the existence of mediation factors that control the relationship between personality traits and cyber-attack victimisation.

With this in mind, our study takes a different approach when dealing with the effects of personality traits on victimisation and proposes that personality traits have indirect effect on user's vulnerability to cyber-attack. There are other factors mediating this relationship such as the individual's competence level, the individual's motivation to use social network's service, the individual's trust in social network's members and provider, and the individual's experience with cyber-crime.

In this context, the present study proposes a mediation model that estimates how personality traits affect those mediation factors and thereby influence the user's likely victimisation. The proposed model has been validated using a partial least squares structural equation modelling technique which allow us to test the relationships between constructs and the mediations' significance.

The rest of this paper is organised as follows. Section II presents a literature review. Section III provides details about the model components and hypotheses. Section IV describes the study methodology while Section V presents the findings of the analysis. Discussion of the results is provided in Section VI and Section VII summarises the results and offers conclusions from the study.

II. LITERATURE REVIEW

Social engineering attacks are a sophisticated attempt to gain access or acquire sensitive information. The goal of such attacks is to target and exploit the users rather than the system. Therefore, investigating user weaknesses and vulnerabilities that prevent them from detecting social engineering attacks is essential to protect against these threats.

Previous cyber-attacks research has extensively focused on human vulnerabilities in email environment. Some of this research proposed models to predict human behaviour toward email phishing. For instance, Alseadoon et al. [5], and Halevi et al. [4] have invistegated different human characteristics such as demographics, trust, and email experience in order to predict the individual detection ability of email phishing. Personality trait is another characteristic which has been assumed to have a direct influence on people's detection ability for email phishing attacks. Despite the similar environment and setting of the two studies, each study had different findings. The inconsistent

results show that there might be other factors controlling this relationship. Personality alone cannot determine human behaviour as there are other important situational-related factors that must be considered in order to predict user reaction [9].

Other research has concentrated on the taxonomy of social engineering attacks and give more details about the type and settings of various attacks which helps to increase awareness of why such attacks are successful. A recent novel social engineering taxonomy has been proposed [6] that classifies social engineering based on the three categories of channel (medium of attack), operator (the attacker), and type (approach of attack). Based on this classification the type of channel can determine the potential type of attacks that occurs on that medium. This means that attacks occurring on social network environments are different than those that usually happen in an email environment. Therefore, previously proposed models for an email environment could be limited if applied to a social network setting which has different challenging and demanding characteristics. This make us also think that even the human characteristics that affect the users' judgment of cyber-attacks in social networks could be different from the factors that are believed to affect people's decision to comply with phishing attacks in an email context.

Limited research has focused on why people are easily tricked by social engineering attacks in the context of social networks. Vishwanath (2016) has investigated the habitual related factors that could affect people's vulnerability to Facebook phishing attacks and found that the desire to increase friendship connections as well as the frequency of network usage have high impact on user behaviour [7]. Saridakis et al (2016) studied perceptual related factors and concluded that people with high risk propensity are more likely to fall victim to cyber-attacks [8]. Furthermore, the earlier study pointed out that engaging in knowledge exchange networks such as 'LinkedIn' is positively related to cyber-attack victimisation when compared to engaging in multi-purpose social network domains such as Facebook. Previous studies have indicated the need to develop a multifaceted model that could predict human vulnerability, particularly in social network environment.

III. THE MEDIATION MODEL OF CYBER-ATTACK SUSCEPTIBILITY

Fig. 1 illustrates our multiple mediation model of the association between the five personality traits and user's susceptibility to cyber-attack in a social network context, via user's competence level, user's trust in social network members and provider, user's motivation to use a social network, and user's past experience with cyber-crime. More detail of the model components and hypotheses will be discussed in the following.

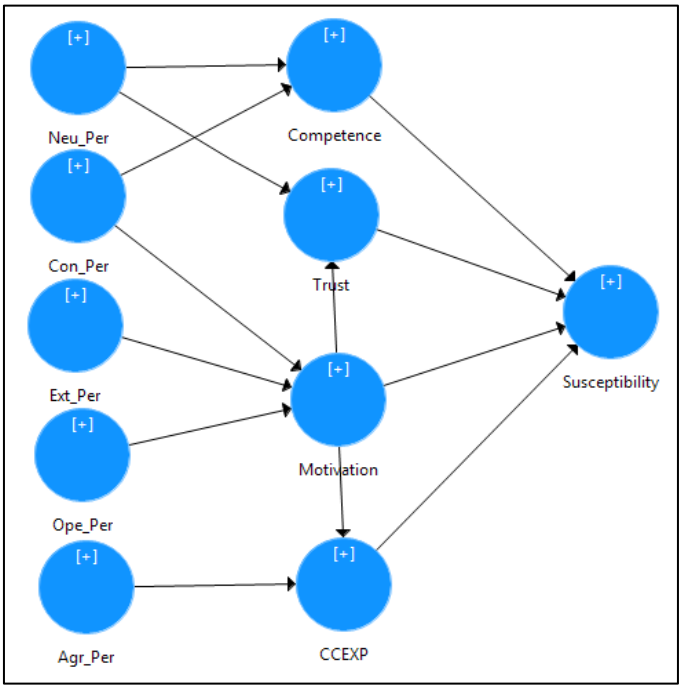

Fig. 1. The study Model

A. *The study mediators*

The proposed model has four mediators which will be explained in this section and their relation to the target variable will be hypothesised.

User competence in dealing with risky situations in social network setting is an important predictor of the user's response to online threats. Self-efficacy, which is one of the user's competence dimensions [10], has been found to play a critical role in user's safe and preservative behaviour online [11]. People who have confidence in their ability to protect themselves online as well as high security awareness can be perceived as highly competent users when facing cyber-attacks [12]. This study hypothesised that highly competent users are less susceptible to cyber-attack victimisation.

Ha1. User's competence decreases the user's susceptibility to cyber-attack victimisation.

In the context of social networks, trust can be derived from members' trust for each other as well as trusting the network provider. Previous research [5], [13] stressed that the disposition to trust is a predictor of the user's probability of being deceived by cyber-attacks. Therefore, we hypothesised that trusting the social network provider as well as their members may cause higher susceptibility to cyber-attacks.

Ha2. Trust increases the user's susceptibility to cyber-attack victimisation.

User's differing motivation to use social networking sites can explain their attitude online, such as disclosing personal information on social networks [14]. Hedonically motivated users who usually seek enjoyment can be persuaded to click on links that provide new games or apps while socially motivated

users are usually looking to meet new people online and make more connections with strangers. This is considered risky behaviour nowadays. Therefore, motivated users are more vulnerable to cyber-attack victimisation than others.

Ha3. Motivation increasers the user's susceptibility to cyber-attack victimisation.

Past victimisation is observed as highly affecting the person's view of happiness and safety in general [15]. Also, this unpleasant experience is inclined to change behaviour, such as reducing the likelihood of engagement in online-shopping [16] or even increasing antisocial behaviour [17]. Furthermore, losing personal information in past phishing attacks is claimed to raise user awareness and thus prevent them from being phished again, but recent study found this claim to be not significant [18]. People past experience with cyber-crimes can be used as a determinant of their weakness to protect themselves from such attacks. Therefore, this study hypothesised that past experience is a predictor of the user's possibility to being victimised again.

Ha4. Past experience with cyber-crimes increases the user's susceptibility to cyber-attack victimisation.

B. The five Personality traits hypotheses

The hypotheses development for the indirect effects of the five personality traits on the user's susceptibility to cyber-attack victimisation will be explained as follow.

1) Conscientiousness

This trait is characterised by high concentration and attention to detail. People with this trait are usually organised and known for their self-control. A previous study [19] reveals a positive relationship between conscientiousness and self-efficacy. Users with high self-efficacy are likely to take control and protect their personal information online [11]. Therefore, our study hypothesised a positive relation between this trait and user competence. People who exhibit conscientiousness have ability to control their desire and manifest low motivation to engage in social networks - as revealed by a recent study [20]. The indirect effect of this trait on susceptibility to cyber-attacks is mediated by the user's competence and motivation and is hypothesised to be negative.

Hb1. Conscientiousness has a negative indirect effect on susceptibility to cyber-attack victimisation that is mediated by competence and motivation.

2) Neuroticism

People with this trait are usually anxious and worry about every step they take [21]. High levels of stress and anxiety usually lead to a decrease in risk-taking behaviour [22]. Neuroticism is also found to increase correct judgment over whether information should be trusted or not and thereby, decreases phishing susceptibility [23]. Consequently, our study hypothesised that this trait has a negative relation to trust and therefore, is negatively related to susceptibility to cyber-attacks. However, this trait is also assumed to be negatively related to user's competence, since dealing with stressful situations is a weakness of neurotic characters.

Hb2. Neuroticism has a negative indirect effect on susceptibility to cyber-attack victimisation that is mediated by trust and competence.

3) Extraversion

People with this trait are usually seen as sociable and attention-seekers. A recent study revealed that people with high extraversion tend to have high motivation to engage in social networks [20]. Extraversion is also found to positively impact the user's willingness to comply with phishing requests [5]. Therefore, it has been predicted that this characteristic will have a positive effect on susceptibility to cyber-attacks and this effect is mediated by the individual's motivation to engage in social networks.

Hb3. Extraversion has a positive indirect effect on susceptibility to cyber-attack victimisation that is mediated by motivation.

4) Agreeableness

People with this trait usually have a disposition to trust others as they are normally kind and like to help. In the context of social networks, agreeable people have a high propensity to self-disclosure [24] which is believed to be risky behaviour leading to possible security and privacy exploitation [25]. Moreover, previous research [26] argued that this aspect of personality is the most strongly related to phishing email victimisation. Therefore, our study predicts a positive relation between this trait and past experience with cyber-crime and also an indirect effect between this trait and victimisation.

Hb4. Agreeableness has a positive indirect effect on susceptibility to cyber-attack victimisation that is mediated by past experience with cyber-crime.

5) Openness to experience

People with this trait have the imagination and the fantasy to explore new experiences. Openness to new experience is positively correlated with risky decisions [22]. A previous study [20] posits that openness to experience is positively related to user's positive attitude toward social networking sites. Therefore, it has been assumed that since their motivation to engage in social networks is high, their susceptibility to cyber-attacks is likely to be high as well.

Hb5. Openness has a positive indirect effect on susceptibility to cyber-attack victimisation that is mediated by motivation.

IV. METHODOLOGY

A scenario-based experiment has been conducted as this method is well suited to cyber-attack studies due to the ethical concerns associated with conducting real attacks. Adopting a scenario-based approach is the closest way to approximate real attacks as users can imagine themselves facing the scenarios in their real accounts and respond accordingly. An invitation

email with the link of the online-based questionnaire was sent to a number of faculty staff in two Saudi universities asking them to disseminate the email among their students and staff. As a result, 316 participants have completed the study. This included both genders, a range of ages between 18 and 55, and different levels of education. The online-based questionnaire includes the measurement scales for the study constructs as well as four pictures of social network (Facebook) posts that present different types of attacks, such as click-jacking and phishing.

The four Facebook posts that have been designed to measure user's susceptibility to cyber-attacks include the social engineering requests. These requests have been chosen carefully based on the most common and spreading social engineering attacks in social networks [27] such as phishing attack that requests sensitive information (Attack 1), clickjacking with executable file (Attack 2), malware attack (Attack 3), and phishing scam that impersonates a legitimate organization (Attack 4). Participants have been presented with the cyber-attack posts and asked to express their behaviour toward these requests if they encountered them in their real account by rating a number of statements such as "I would click on this link", or "I would register my name and email to win" using a 5 point Likert scale (from strongly disagree to strongly agree).

The measurement scales used in the study are mostly adopted from previous literature, such as personality test [28], motivation [29], trust [30], [31], past experience [16], and competence [10]. Due to its suitability with developing theories and prediction models [32], a partial least squares (PLS) path modelling approach is used to estimate the model relationships. SmartPLS 3 software package [33] has been used to analyse the study model.

V. RESULTS

Before examining the mediation effects, we must first see if the mediators have significant effect on user's susceptibility to cyber-attacks victimisation. Table 1 provides the results of the significance test of the mediators on the target variable. T statistics from a bootstrap procedure are presented along with the relationships' paths which indicate a significant path if the t value is greater than the threshold of 1.96. All the mediators positively and significantly influence the user's susceptibility except competence, which has a significant negative effect (β= -0.148). Furthermore, trust has the highest influence on the user's likelihood of falling victim (t=6.344, p<0.01), followed by the usage motivation (t=4.401, p<0.01), and past victimisation (t=4.340, p<0.01) while user competence has the lowest effect (t=2.757, p<0.01).

TABLE 1. BOOTSTRAPPING TOTAL EFFECT OF MEDIATORS ON USER'S SUSCEPTIBILITY

H	Relationship	β	SE	t	p	Decision
Ha1	Comp-> Suscept	-0.148	0.054	2.757	0.006	Supported
Ha2	Trust -> Suscept	0.361	0.057	6.344	0.000	Supported
Ha3	Mot -> Suscept	0.206	0.047	4.401	0.000	Supported
Ha4	CCEXP -> Suscept	0.261	0.060	4.340	0.000	Supported

Table 2 summarises the bootstrapping analysis of the total indirect effect for all the personality traits on the user's susceptibility to cyber-attacks. Openness is the only trait that appeared to have no effect on the user's vulnerability (t=0.989) as the confidence interval for this relation includes zero. Openness mediation path will not be examined in the next table as one of the mediation conditions has not been met, i.e., the total effect between IV and DV must be significant. We also found that agreeableness has a significant negative effect on users' susceptibility to cyber-attacks; a conclusion that is contrary to our hypothesis. Extraversion is the personality trait that has the strongest significant effect on user's susceptibility to cyber-attack (t=3.223, p<0.01) followed by conscientiousness (t=3.163, p<0.01).

TABLE 2. BOOTSTRAPPING TOTAL INDIRECT EFFECTS OF PERSONALITY TRAITS ON USER'S SUSCEPTIBILITY

H	Relationship	β	t	95% Confidence interval		Decision
				2.5%	97.5%	
Hb1	Con_per -> Suscept	-0.059	3.163	-0.103	-0.028	Supported**
Hb2	Neu_per -> Suscept	-0.051	2.021	-0.104	-0.004	Supported*
Hb3	Ext_per -> Suscept	0.055	3.223	0.026	0.093	Supported**
Hb4	Agr_Per -> Suscept	-0.040	2.333	-0.083	-0.013	Supported*
Hb5	Ope_per -> Suscept	0.012	0.989	-0.010	0.040	Rejected

Significant at **P= < 0.01, *P <0.05

The PLS bootstrapping results in Table 2 show the total indirect effect for the independent variables (personality traits) on the dependent variable (susceptibility to cyber-attack) including all mediators' effect in the model. Yet, in order to determine each mediator effect alone on a specific relationship, the recommendations of Hair et al. (2017) [34] have been followed to calculate specific indirect effects and the mediation type has been identified according to the typology of mediations that has been proposed by Zhao et al. (2010) [35].

Table 3 shows the result of the specific mediation path of every mediator between the personality traits and user's susceptibility to cyber-attack victimisation. Some mediators are found to have no mediation effect when treating them as the only mediator between a specific relationship such as motivation either between extraversion or conscientiousness and the user's susceptibility to cyber-attack. Yet, motivation jointly with trust has significant serial mediation effects on the earlier relationships, as supported by the 95% confidence interval. All other mediations paths have indirect only mediation effects between the personality traits and the target variable. Competence is the strongest mediator between conscientiousness and cyber-attack susceptibility (t=2.157, p<0.05). While, trust plays a significant mediation role on the relationship between neuroticism and cyber-attack victimisation, with t=3.551; p=0.00. Past experience is the only mediation between agreeableness and susceptibility to victimisation which proved to be significant, with t=2.386.

TABLE 3. MULTIPLE MEDIATION TEST

Relationship	β	SE	t	p	95% CI	Mediation Type
Con_per -> Suscept via Comp	-0.033	0.015	2.157	0.031	[-0.062, -0.003]	indirect only
Con_per -> Suscept via Mot	-0.005	0.007	0.737	0.461	[-0.020, 0.009]	no effect
Neu_per -> Suscept via Comp	0.029	0.013	2.198	0.028	[0.003, 0.054]	indirect only
Neu_per -> Suscept via Trust	-0.080	0.023	3.551	0.000	[-0.124, -0.036]	indirect only
Agr_Per -> Suscept via CCEXP	-0.040	0.017	2.386	0.017	[-0.072, -0.007]	indirect only
Ext_per -> Suscept via Mot	0.011	0.013	0.847	0.398	[-0.015, 0.038]	no effect
Ext_per -> Suscept via Mot+Trust	0.030	0.009	3.261	0.001	[0.012, 0.048]	serial mediation
Con_per -> Suscept via Mot+Trust	-0.014	0.007	2.083	0.038	[-0.028, -0.001]	serial mediation

VI. DISCUSSION

Conscientiousness in personality is always associated with self-control as well as high concentration, which make users with this personality trait keen to protect themselves from potential online threats. We found that this trait is strongly and negatively related to social network's threat victimisation. The result accords with previous findings [36], that low impulsive people are better and more effective in dealing with phishing emails. Conscientiousness in personality is also associated with high information security awareness [37], rules commitment [38] and willingness to use security software [39], which also supports our findings that people with this personality trait are normally less susceptible to cyber-crimes.

People with neuroticism in their personality usually have difficulty in dealing with stressful situations which make them less able to protect themselves from online threats. Halevi et al's study [4] supports this finding as it found that neurotic women are more vulnerable to phishing. Yet, highly neurotic people tend to be over concerned about everything which makes them less trusting. We found that the relationship between neuroticism and trust ($t = -4.464$) is stronger than the relationship between neuroticism and competence ($t = -3.228$), which supports the final result that even if people with neuroticism in their personality might be not competent enough, their lack of trust on other people makes them less vulnerable to social network threats.

The tendency to extraversion is the personality characteristic that makes users most vulnerable to cyber-attack victimisation on social networking sites such as Facebook. The result of the present study revealed that this personality trait is the only one positively associated with cyber-attack victimisation. This finding agrees with a previous study [5] that high level of extraversion increases people's tendency to obey and respond to email phishing requests. Yet, this result contradicts another empirical study [36] that indicated that people with extraversion personality are highly effective in dealing with phishing emails. However, it is important to note that the earlier study has some sample limitation, N=59.

People with a high level of agreeableness are inclined to help others in need and are known to be kind, and cooperative. Therefore, based on previous study results [5], this study hypothesised that individuals with agreeableness as a personality trait are more likely to fall for cyber-attacks. Yet, the result of our study indicated that agreeableness decreases the user's susceptibility to cyber-attacks. This result can be seen as contrary to common sense but interesting, as agreeable people had low past victimisation experience ($t = -2.820$) and thereby a negative relationship ($t = -2.333$, $p < 0.05$) with cyber-attack vulnerability. This result also accords with a previous study [39] that people with agreeableness are more likely to adopt security software than other users. Agreeable users usually follow organizations' rules and show high commitment and integrity in their work place [38]. Furthermore, agreeable individuals showed high information security awareness [37] as well as great efficiency in detecting phishing attack, in a previous study [23]. This might explain our result since agreeable users could be following security and privacy rules in social network and therefore be less vulnerable to cyber-attack victimisation.

Finally, a previous study [5] revealed that people with high openness-to-experience personality are more likely to respond to email phishing. Yet, another study [36] detects the opposite relationship, where the more open the user the better performance they will show in dealing with phishing emails. However, our result showed that openness has no direct or mediated effect on user's susceptibility. A result that also agrees with a previous study [4] that found no relation between openness and email phishing victimisation.

VII. CONCLUSION

Personality traits are considered important predictors of human behaviour in information security research. Yet, previous studies that treat them as having direct effects on the dependent variables often conclude with conflict and inconsistant results. The present study found personality traits to be significant predictors of human vulnerability to cyber-attacks. Yet, these relations are indirect and mediated by other important factors. The study result demonstrates that users' trust, competence, motivation, and past experience with cyber-crimes play an important role in explaining the influence of the five personality traits on susceptibility to cyber-attacks in social networks. Conscientiousness, agreeableness, and neuroticism are found to strongly decrease the user's susceptibility to cyber-attacks in social network settings. While extraversion is found to significantly increase the user's likelihood of falling victim to cyber-attacks.

One limitation of this study is that using self-reported personality test may not precisely reflect the individual's real personality, as people sometimes behave differently based on other stimuli. Further efforts are needed in this area, as predicting human behaviour is a complex task. The present study offers a basis for investigating the impact of personality traits as antecedents of other exogenous factors that affect human vulnerability to cyber-attack.

REFERENCES

[1] P. Costa and R. McCrae, "Four ways five factors are basic," *Pers. Individ. Dif.*, vol. 13, no. 6, pp. 653–665, 1992.

[2] L. Lin, "The relationship of consumer personality trait, brand personality, and brand loyalty: an empirical study of toys and video games buyers," *J. Prod. Brand Manag.*, vol. 19, no. 1, pp. 4–17, 2010.

[3] M. Caliendo, F. Fossen, and A. Kritikos, "Personality Characteristics and the Decision to Become and Stay Self-Employed," *SOEP Pap.*, no. March 2011.

[4] T. Halevi, J. Lewis, and N. Memon, "Phishing, Personality Traits and Facebook," *arXiv Prepr. arXiv1301.7643.*, 2013.

[5] I. Alseadoon, M. F. I. 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*, Springer International Publishing, 2015, pp. 949–962.

[6] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, 2015.

[7] A. Vishwanath, "Habitual facebook use and its impact on getting deceived on social media," *J. Comput. Commun.*, vol. 20, no. 1, pp. 83–98, 2015.

[8] G. Saridakis, V. Benson, J. N. Ezingeard, and H. Tennakoon, "Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users," *Technol. Forecast. Soc. Change*, vol. 102, pp. 320–330, 2016.

[9] E. T. Higgins, "Does personality provide unique explanations for behaviour? Personality as cross-person variability in general principles," *Eur. J. Pers.*, vol. 14, no. 5, pp. 391–406, 2000.

[10] S. M. Albladi and G. R. S. Weir, "Competence Measure in Social Networks," in *The 51st International Carnahan Conference on Security Technology*, 2017.

[11] G. R. Milne, L. I. Labrecque, and C. Cromer, "Toward an understanding of the online consumer's risky behavior and protection practices," *J. Consum. Aff.*, vol. 43, no. 3, pp. 449–473, 2009.

[12] R. T. Wright and K. Marett, "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *J. Manag. Inf. Syst.*, vol. 27, no. 1, pp. 273–303, 2010.

[13] M. Workman, "A test of interventions for security threats from social engineering," *Inf. Manag. Comput. Secur.*, vol. 16, no. 5, pp. 463–483, 2008.

[14] C. W. Chang and J. Heo, "Visiting theories that predict college students' self-disclosure on Facebook," *Comput. Human Behav.*, vol. 30, pp. 79–86, 2014.

[15] S. Mahuteau and R. Zhu, "Crime Victimisation and Subjective Well-Being: Panel Evidence From Australia," *Heal. Econ. (United Kingdom)*, vol. 25, no. 11, pp. 1448–1463, 2016.

[16] B. Rainer and T. Moore, "How Do Consumers React to Cybercrime ?," in *eCrime Researchers Summit (eCrime)*, 2012, pp. 1–12.

[17] B. Cao and W. Y. Lin, "How do victims react to cyberbullying on social networking sites? The influence of previous cyberbullying victimization experiences," *Comput. Human Behav.*, vol. 52, pp. 458–465, 2015.

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

[19] L. Di Giunta, G. Alessandri, M. Gerbino, P. Luengo Kanacri, A. Zuffiano, and G. V. Caprara, "The determinants of scholastic achievement: The contribution of personality traits, self-esteem, and academic self-efficacy," *Learn. Individ. Differ.*, vol. 27, pp. 102–108, 2013.

[20] Y. P. Chua and Y. P. Chua, "Do computer-mediated communication skill, knowledge and motivation mediate the relationships between personality traits and attitude toward Facebook?," *Comput. Human Behav.*, vol. 70, pp. 51–59, 2017.

[21] R. J. Taormina and R. Sun, "Antecedents and Outcomes of Psychological Insecurity and Interpersonal Trust Among Chinese People," *Psychol. Thought*, vol. 8 (2), no. 2015, pp. 173–188, 2015.

[22] M. Lauriola and I. P. Levin, "Personality traits and risky decision-making in a controlled experimental task: An exploratory study," *Pers. Individ. Dif.*, vol. 31, no. 2, pp. 215–226, 2001.

[23] J. H. Cho, H. Cam, and A. Oltramari, "Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis," *2016 IEEE Int. Multi-Disciplinary Conf. Cogn. Methods Situat. Aware. Decis. Support. CogSIMA 2016*, pp. 7–13, 2016.

[24] G. Seidman, "Self-presentation and belonging on Facebook: How personality influences social media use and motivations," *Pers. Individ. Dif.*, vol. 54, no. 3, pp. 402–407, 2013.

[25] A. Nosko, E. Wood, and S. Molema, "All about me: Disclosure in online social networking profiles: The case of FACEBOOK," *Comput. Human Behav.*, vol. 26, no. 3, pp. 406–418, 2010.

[26] J. L. Parrish Jr., J. L. Bailey, and J. F. Courtney, "A Personality Based Model for Determining Susceptibility to Phishing Attacks," in *Southwest Decision Sciences Institute (SWDSI) annual meeting*, 2009, no. July 2015, pp. 285–296.

[27] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 56–63, 2011.

[28] B. Rammstedt and O. P. John, "Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German," *J. Res. Pers.*, vol. 41, no. 1, pp. 203–212, 2007.

[29] P. B. Brandtzaeg and J. Heim, "Why People Use Social Networking Sites," in *International Conference on Online Communities and Social Computing*, 2009, pp. 143–152.

[30] J. Fogel and E. Nehmad, "Internet social network communities : Risk taking , trust , and privacy concerns," *Comput. Human Behav.*, vol. 25, no. 1, pp. 153–160, 2009.

[31] C. M. Chiu, M. H. Hsu, and E. T. G. Wang, "Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories," *Decis. Support Syst.*, vol. 42, no. 3, pp. 1872–1888, 2006.

[32] J. Henseler, C. M. Ringle, and R. R. Sinkovics, "The use of partial least squares path modeling in international marketing," *Adv. Int. Mark.*, vol. 20, no. 1, pp. 277–319, 2009.

[33] C. M. Ringle, S. Wende, and J.-M. Becker, "SmartPLS 3." Bönningstedt: SmartPLS, 2015.

[34] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd Ed. Thousand Oaks: Sage, 2017.

[35] X. Zhao, J. G. Lynch, and Q. Chen, "Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis," *J. Consum. Res.*, vol. 37, no. 2, pp. 197–206, 2010.

[36] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius, "Why do some people manage phishing e-mails better than others?," *Inf. Manag. Comput. Secur.*, vol. 20, no. 1, pp. 18–28, 2014.

[37] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Comput. Human Behav.*, vol. 69, pp. 151–156, 2017.

[38] R. P. Guay, D. Choi, I. S. Oh, M. S. Mitchell, M. K. Mount, and K. H. Shin, "Why people harm the organization and its members: Relationships among personality, organizational commitment, and workplace deviance," *Hum. Perform.*, vol. 29, no. 1, pp. 1–15, 2016.

[39] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Comput. Secur.*, vol. 49, pp. 177–191, 2015.