Albladi and Weir *Cybersecurity* (2020) 3:7
https://doi.org/10.1186/s42400-020-00047-5

Cybersecurity

RESEARCH Open Access

Predicting individuals' vulnerability to social engineering in social networks

Samar Muslah Albladi[1*] and George R. S. Weir[2]

Abstract

The popularity of social networking sites has attracted billions of users to engage and share their information on these networks. The vast amount of circulating data and information expose these networks to several security risks. Social engineering is one of the most common types of threat that may face social network users. Training and increasing users' awareness of such threats is essential for maintaining continuous and safe use of social networking services. Identifying the most vulnerable users in order to target them for these training programs is desirable for increasing the effectiveness of such programs. Few studies have investigated the effect of individuals' characteristics on predicting their vulnerability to social engineering in the context of social networks. To address this gap, the present study developed a novel model to predict user vulnerability based on several perspectives of user characteristics. The proposed model includes interactions between different social network-oriented factors such as level of involvement in the network, motivation to use the network, and competence in dealing with threats on the network. The results of this research indicate that most of the considered user characteristics are factors that influence user vulnerability either directly or indirectly. Furthermore, the present study provides evidence that individuals' characteristics can identify vulnerable users so that these risks can be considered when designing training and awareness programs.

Keywords: Deception, Information security, Phishing, Social engineering, Social network, Vulnerability

Introduction

Individuals and organisations are becoming increasingly dependent on working with computers, accessing the Internet, and more importantly sharing data through virtual communications. This makes cybersecurity one of today's most significant issues. Protecting people and organisations from being targeted by cybercriminals is becoming a priority for industry and academia (Gupta et al. 2018). This is due to the substantial damage that may result from losing valuable data and documents in such attacks. Rather than exploiting technical means to reach their victims, cybercriminals may instead use deceptive social engineering (SE) strategies to convince their targets to accept the lure. Social engineers exploit individuals motives, habits, and behaviour to manipulate their victims (Mitnick and Simon 2003).

Often, security practitioners still rely on technical measures to protect from online threats while overlooking the fact that cybercriminals are targeting human weak points to spread and conduct their attacks (Krombholz et al. 2015). According to the human-factor report (Proofpoint 2018), the number of social engineering attacks that exploit human vulnerabilities dramatically increased over the year examined. This raises the necessity of finding a solution that helps the user toward acceptable defensive behaviour in the social network (SN) setting. Identifying the user characteristics that make them more or less vulnerable to social engineering threats is a major step toward protecting against such threats (Albladi and Weir 2018). Knowing where weakness resides can help focus

* Correspondence: Salbladi@uj.edu.sa
[1]College of Computer Science and Engineering, University of Jeddah, Jeddah, Kingdom of Saudi Arabia
Full list of author information is available at the end of the article

awareness-raising and target training sessions for those individuals, with the aim of reducing their likely victimisation.

With such objectives in mind, the present research developed a conceptual model that reflects the extent to which the user-related factors and dimensions are integrated as a means to predict users' vulnerability to social engineering-based attacks. This study used a scenario-based experiment to examine the relationships between the behavioural constructs in the conceptual model and the model's ability to predict user vulnerability to SE victimisation.

The organisation of this paper is as follows: Theoretical background section briefly analyses the related literature that was considered in developing the proposed model. The methods used to evaluate this model are described in Methods section. Following this, the results of the analysis are summarised in Results section. Discussion section provides a discussion of the findings while Theoretical and practical implications section presents the theory and practical implications. An outline approach to a semi-automated advisory system is proposed in A semi-automated security advisory system section. Finally, Conclusion section draws conclusions from this work.

Theoretical background

People's vulnerability to cyber-attacks, and particularly to social engineering-based attacks, is not a newly emerging problem. Social engineering issues have been studied in email environments (Alseadoon et al. 2015; Halevi et al. 2013; Vishwanath et al. 2016), organisational environments (Flores et al. 2014, 2015), and recently in social network environments (Algarni et al. 2017; Saridakis et al. 2016; Vishwanath 2015). Yet, the present research argues that the context of these exploits affects peoples' ability to detect them, and that the influences create new characteristics and elements which warrant further investigation.

The present study investigated user characteristics in social networks, particularly Facebook, from different angles such as peoples' behaviour, perceptions, and socio-emotions, in an attempt to identify the factors that could predict individuals' vulnerability to SE threats. People's vulnerability level will be identified based on their response to a variety of social engineering scenarios. The following sub-sections will address in detail the relationship between each factor of the three perspectives and user susceptibility to SE victimisation.

Habitual perspective

Due to the importance of understanding the impact of peoples' habitual factors on their susceptibility to SE in SNs, this study aims to measure the effect of level of involvement, number of SN connections, percentage of known friends among the network's connections, and SN experience on predicting user susceptibility to SE in the conceptual model.

Level of involvement

This construct is intended to measure the extent to which a user engages in Facebook activities. When people are highly involved with a communication service, they tend to be relaxed and ignore any cues associated with such service that warn of deception risk (Vishwanath et al. 2016). User involvement in a social network can be measured by the number of minutes spent on the network every day and the frequency of commenting on other people's status updates or pictures (Vishwanath 2015). Time spent on Facebook is positively associated with disclosing highly sensitive information (Chang and Heo 2014). Furthermore, people who are more involved in the network are believed to be more exposed to social engineering victimisation (Saridakis et al. 2016; Vishwanath 2015).

Conversely, highly involved users are supposed to have more experience with the different types of threat that could occur online. Yet, it has been observed that active Facebook users are less concerned about sharing their private information as they usually have less restrictive privacy settings (Halevi et al. 2013). Users' tendency to share private information could relate to the fact that individuals who spend a lot of time using the network usually exhibit high trust in the network (Sherchan et al. 2013). Therefore, the following hypotheses have been proposed.

- **Ha1.** Users with a higher level of involvement will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).
  - **Hb1.** The user's level of involvement positively influences the user's experience with cybercrime.
  - **Hb2.** The user's level of involvement positively influences the user's trust.

Number of connections

Despite of the fact that having large number of SN connections could increase people's life satisfaction if they are motivated to engage in the network to maintain friendships (Rae and Lonborg 2015), this high number of contacts in the network is claimed to increase vulnerability to online risks (Buglass et al. 2016; Vishwanath 2015). Risky behaviour such as disclosing personal information in Facebook is closely associated with users' desire to maintain and increase the number of existing friends (Chang and Heo 2014; Cheung et al. 2015). Users with a high number of social network connections are motivated to be more involved in the network by spending more time sharing information and maintaining their profiles (Madden et al. 2013).

Furthermore, a high number of connections might suggest that users are not only connected with their friends but also with strangers. Vishwanath (2015) has claimed that connecting with strangers on Facebook can be considered as the first level of cyber-attack victimisation, as those individuals are usually less suspicious of the possible threats that can result from connecting with strangers in the network. Furthermore, Alqarni et al. (2016) have adopted this view to test the relationship between severity and vulnerability of phishing attacks and connection with strangers (as assumed to present the basis for phishing attacks). Their study indicated a negative relationship between the number of strangers that the user is already connected to and the user's perception of the severity and their vulnerability to phishing attacks in Facebook. Therefore, if users are connected mostly with known friends on Facebook, this could be seen as a mark of less vulnerable individuals. With all of these points in mind, the following hypotheses are generated.

- **Ha2:** Users with a higher number of connections will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).
  - **Hb3:** The user's number of connections positively influences the user's level of involvement.
- **Ha3:** Users with higher connections with known friends will be less susceptible to social engineering attacks (i.e., there will be a negative relationship).

Social network experience

People's experience in using information communication technologies makes them more competent to detect online deception in SNs (Tsikerdekis and Zeadally 2014). For instance, it has been found that the more time elapsed since joining Facebook makes the user more capable of detecting SE attacks (Algarni et al. 2017). Furthermore, despite the fact that some researchers argue that computer experience has no significant impact on their phishing susceptibility (Halevi et al. 2013; Saridakis et al. 2016), other research on email phishing found positive impact from number of years of using the Internet and number of years of using email on people's detection ability with email phishing (Alseadoon 2014; Sheng et al. 2010). Therefore, the present study suggests that the more experienced are the users with SNs, the less vulnerable they are to SE victimisation.

Additionally, in the context of the social network, Internet experience has been found to predict precautionary behaviour, and further causes greater sensitivity to associated risks in using Facebook (Van Schaik et al. 2018). Thus, years of experience in using the network could increase the individual's awareness of the risk associated with connecting with strangers. Accordingly, the present study postulates that more experienced users would have a high percentage of connections with known friends in the network.

- **Ha4:** Users with a higher level of experience with social network will be less susceptible to social engineering attacks (i.e., there will be a negative relationship).
  - **Hb4:** The user's social network experience positively influences the user's connections with known friends.

Perceptual perspective

People's risk perception, competence, and cybercrime experience are the three perceptual factors that are believed to influence their susceptibility to social engineering attacks. The strength and direction of these factors' impact will be discussed as follows.

Risk perception

Facebook users have a different level of risk perception that might affect their decision in times of risk. Vishwanath et al. (2016) has described risk perception as the bridge between user's previous knowledge about the expected risk and their competence to deal with that risk. Many studies have considered perceiving the risk associated with engaging in online activities as having a direct influence on avoiding using online services (Riek et al. 2016) and more importantly as decreasing their vulnerability to online threats (Vishwanath et al. 2016). Facebook users' perceived risk of privacy and security threats significantly predict their strict privacy and security settings (Van Schaik et al. 2018). Thus, if online users are aware of the potential risks and their consequences that might be encountered on Facebook, they will probably avoid clicking on malicious links and communicating with strangers on the network. This indicates that risk perception contributes to the user's competence in dealing with online threats and should lead to a decrease in susceptibility to SE. Therefore, the following relationships have been proposed.

- **Ha5:** Users with a higher level of risk perception will be less susceptible to social engineering attacks (i.e., there will be a negative relationship).
  - **Hb5:** The user's perceived risk positively influences the user's competence.

Competence

User competence has been considered an essential determinant of end-user capability to accomplish tasks in many different fields. In the realm of information systems, user competence can be defined as the individual's knowledge of the intended technology and ability to use it effectively (Munro et al. 1997). To gain insight into user competence in detecting security threats in the context of online social networks, investigating the multidimensional space that determines this user competence level is fundamental (Albladi and Weir 2017). The role of user competence and its dimensions in facilitating the detection of online threats is still a controversial topic in the information security field. The dimensions used in the present study to measure the concept are security awareness, privacy awareness, and self-efficacy. The scales used to measure these factors can determine the level of user competence in evaluating risks associated with social network usage.

User competence in dealing with risky situations in a social network setting is a major predictor of the user's response to online threats. When individuals feel competent to control their information in social networks, they are found to be less vulnerable to victimisation (Saridakis et al. 2016). Furthermore, Self-efficacy, which is one of the user's competence dimensions, has been found to play a critical role in users' safe and preservative behaviour online (Milne et al. 2009). People who have confidence in their ability to protect themselves online as well as having high-security awareness can be perceived as highly competent users when facing cyber-attacks (Wright and Marett 2010). This study hypothesised that highly competent users are less susceptible to SE victimisation.

- **Ha6:** Users with a higher level of competence will be less susceptible to social engineering attacks (i.e., there will be a negative relationship).

Cybercrime experience

Past victimisation is observed as profoundly affecting the person's view of happiness and safety in general (Mahuteau and Zhu 2016). Also, such unpleasant experience is inclined to change behaviour, for example, reducing the likelihood of engagement in online-shopping (Bohme and Moore 2012) or even increasing antisocial behaviour (Cao and Lin 2015). Furthermore, previous email phishing victimisation is claimed to raise user awareness and vigilance and thus prevent them from being victimised again (Workman 2007). Yet, recent studies found this claim to be not significant (Iuga et al. 2016; Wang et al. 2017). As experience with cybercrimes could also be used as a determinant of people's weakness in protecting themselves from such threats.

Experience with cybercrime has been found to increase people's perceived risk of social network services (Riek et al. 2016). Those who are knowledgeable and have previous experience with online threats could be assumed to have high-risk perception (Vishwanath et al. 2016). However, unlike the context of email phishing, little is known about the role of prior knowledge and experiences with cybercrime in preventing people from being vulnerable to social engineering attacks in the context of social networks. Thus, this study proposes that past experience could raise the user's risk perception but also could be used as a predictor of the user's risk of being victimised again. To this extent, the following hypotheses have been assumed.

- **Ha7:** Users with a previous experience with cybercrime will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).
  - **Hb6:** The user's experience with cybercrime positively influences the user's perceived risk.

Socio-emotional perspective

Little is known regarding the impact that this perspective has on SE victimisation in a SN context. However, previous research has highlighted the positive effect of people's general trust or belief in their victimisation in email phishing context (Alseadoon et al. 2015), which encourages the present study to investigate more socio-emotional factors such as the dimensions of user trust and motivation, in order to consider their possible impact on user's risky behaviour.

Trust

Some studies in email phishing (e.g., Alseadoon et al. 2015; Workman 2008) stress that the disposition to trust is a predictor of the user's probability of being deceived by cyber-attacks. In the context of social networks, trust can be derived from the members' trust for each other as well as trusting the network provider. These two dimensions of trust have been indicated to negatively influence people's perceived risk in disclosing personal information (Cheung et al. 2015). Trust has also been found to strongly increase disclosing personal information among social networks users (Beldad and Hegner 2017; Chang and Heo 2014). With all of this in mind, the present study hypothesised that trusting the social network provider as well as other members may cause higher susceptibility to cyber-attacks.

- **Ha8:** Users with a higher level of trust will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).

Motivation

According to the uses and gratification theory, people are using the communication technologies that fulfil their needs (Joinson 2008). Users' motivation to use communication technologies must be taken into consideration in order to understand online user behaviour. This construct has been acknowledged by researchers in many fields such as marketing (Chiu et al. 2014), and mobile technology (Kim et al. 2013) in order to understand their target users. However, information security research has limitedly adopted this view toward understanding the online users' risky behaviour. Users can be motivated by different stimuli to engage in social networks such as entertainment or information seeking (Basak and Calisir 2015). Additionally, people use Facebook for social reasons such as maintaining existing relationships and making new friends (Rae and Lonborg 2015). According to SE victimisation, these motivations can shed light on understanding the user's behaviour at times of risk. For example, hedonically motivated users who usually seek enjoyment are assumed to be persuaded to click on links that provide new games or apps. While socially motivated users are generally looking to meet new people online, this makes them more likely to connect with strangers. This connections with strangers is considered risky behaviour nowadays (Alqarni et al. 2016). Therefore, this study predicts that the users' vulnerability to social engineering-based attacks will be different based on their motives to access the social network.

User's differing motivation to use social networking sites can explain their attitude online, such as tendency to disclose personal information in social networks (Chang and Heo 2014). Additionally, people's perceived benefit of network engagement has a positive impact on their willingness to share their photos online (Beldad and Hegner 2017). Thus, the present study assumes that motivated users are more vulnerable to SE victimisation than others. Additionally, motivated users could be inclined to be more trusting when using technology (Baabdullah 2018). This motivation could lead the individual to spend more time and show higher involvement in the network (Ross et al. 2009). This involvement could ultimately lead motivated individuals to experience or at least be familiar with different types of cybercrime that could happen in the network. Hence, the following hypotheses have been postulated.

- **Ha9:** Users with a higher level of motivation will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).
  - **Hb7:** The user's motivation positively influences the user's trust.
  - **Hb8:** The user's motivation positively influences the user's level of involvement.
  - **Hb9:** The user's motivation positively influences the user's experience with cybercrime.

The previous sub-sections explain the nature and the directions of the relationships among the constructs in the present study. Based on these 18 proposed hypotheses, a novel conceptual model has been developed and presented in Fig. 1. This conceptual model relies on three different perspectives which are believed to predict user behaviour toward SE victimisation on Facebook. Developing and validating such a holistic model gives a clear indication of the contribution of the present study.

Methods

To evaluate the hypotheses of the conceptual model, an online-questionnaire was designed using the Qualtrics online survey tool. The questionnaire incorporated three main parts starting with questions about participants' demographics, followed by questions that measure the constructs of the proposed model, and finally, a scenario-based experiment. An invitation email was sent to a number of faculty staff in two universities, asking them to distribute the online-questionnaire among their students and staff.

Sample

Hair et al. (2017) suggested using a sophisticated guideline that relies on Cohen (1988) recommendations to calculate the required sample size by using power estimates. In this case, for 9 predictors (which is the number of independent variables in the conceptual model) with an estimated medium effect size of 0.15, the target sample size should be at least 113 to achieve a power level of 0.80 with a significance level of 0.05 (Soper 2012). In this study, 316 participants have completed the questionnaire (after the primary data screening). The descriptive analysis of participants' demographics in Table 1 revealed a variety of profiles in terms of gender (39% male, 61% female), education level, and education major. The

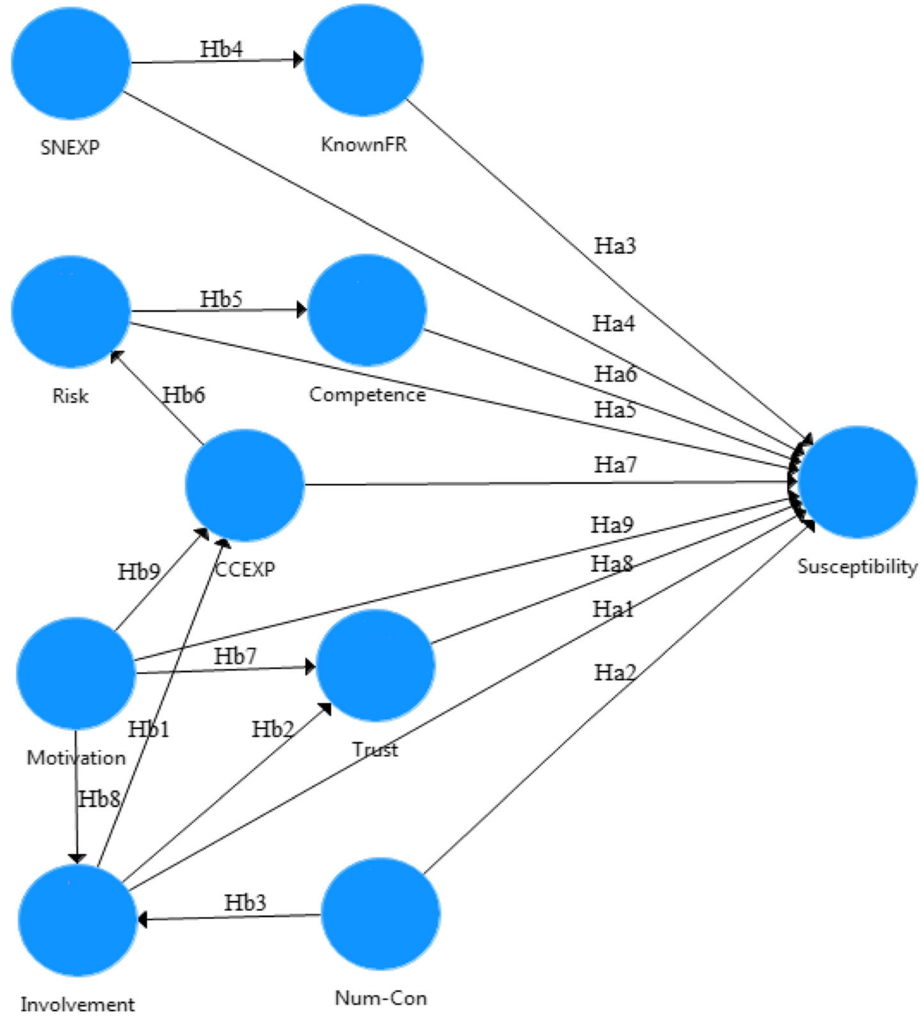

Fig. 1 Research Model

majority of participants in the study were younger adults (age 18–24), representing 76% of the total participants. However, this was expected as the survey was undertaken in two universities where students considered vital members of the higher education environment.

Measurement scales

The proposed conceptual model includes five reflective factors and four second-order formative constructs which are risk, competence, trust, and motivation. Repeated indicator approach was used to measure the formative constructs values. This method recommends using the same number of items on all the first order factors in order to guarantee that all first-order factors have the same weight on the second order factors and to ensure no weight bias are existed (Ringle et al. 2012).

The scales used to measure the user habits in SN has been adopted from (Fogel and Nehmad 2009). To measure the risk perception dimensions, scales were adapted from Milne et al. (2009), with some modification and changes to fit the present study context. The scales used to measure the three dimensions of user competence were adopted from Albladi and Weir (2017). Motivation dimension items were adopted from previous literature (Al Omoush et al. 2012; Basak and Calisir 2015; Orchard et al. 2014; Yang and Lin 2014). The scale used to measure users' trust was adopted with some modification from Fogel and Nehmad (2009) and Chiu et al. (2006) studies. Appendix 1 presents a summary of the measurement items.

A scenario-based experiment has been chosen as an empirical approach to examining users' susceptibility to SE victimisation. In such scenario-based experiments, the human is recruited to take a role in reviewing a set of scripted information which can be in the form of text or images, then asked to react or respond to this predetermined information (Rungtusanatham et al. 2011). This method is considered suitable and realistic for many social engineering studies

Table 1 Participants' demographics

Demographic	Frequency	Percent	Cumulative Percent
Gender			
Male	123	38.9	38.9
Female	193	61.1	100.0
Total	316	100.0	
Age			
18–24	240	75.9	75.9
25–34	57	18.0	94.0
35–44	14	4.4	98.4
45–55	5	1.6	100.0
Total	316	100.0	
Education Level			
High school	187	59.2	59.2
Bachelor's degree	112	35.4	94.6
Master's degree	14	4.4	99.1
Other, please specify	3	.9	100.0
Total	316	100.0	
Major			
Computer Science/IT	124	39.2	39.2
Engineering	32	10.1	49.4
Business/Administrative Sciences	38	12.0	61.4
Medical Sciences	5	1.6	63.0
Science	15	4.7	67.7
Humanities and Arts	6	1.9	69.6
Other, please specify	96	30.4	100.0
Total	316	100.0	

(e.g., (Algarni et al. 2017; Iuga et al. 2016)) due to the ethical concerns associated with conducting real attacks. Our scenario-based experiment includes 6 images of Facebook posts (4 high-risk scenarios, and 2 low-risk scenarios). Each post contains a type of cyber-attack which has been chosen from the most prominent cyber-attacks that occur in social networks (Gao et al. 2011).

In the study model, only high-risk scenarios (which include phishing, clickjacking with an executable file, malware, and phishing scam) have been considered to measure user susceptibility to SE attacks. However, comparing individuals' response to the high-risk attacks and their response to the low-risk attacks aims to examine if users rely on their characteristics when judging the different scenarios and not on other influencing factors such as visual message triggers (Wang et al. 2012). Participants were asked to indicate their response to these Facebook posts, as if they had encountered them in their real accounts, by rating a number of statements such as "I would click on this button to read the file" using a 5-point Likert-scale from 1 "strongly disagree" to 5 "strongly agree". Appendix 2 includes a summary of the scenarios used in this study.

Analysis approach

To evaluate the proposed model, partial least squares structural equation modelling (PLS-SEM) has been used due to its suitability in dealing with complex predictive models that consist in a combination of formative and reflective constructs (Götz et al. 2010), even with some limitations regarding data normality and sample size (Hair et al. 2012). The SmartPLS v3 software package (Ringle et al. 2015) was used to analyse the model and its associated hypotheses.

To evaluate the study model, three different procedures have been conducted. First, using the PLS-algorithm to provide standard model estimations such as path coefficient, the coefficient of determination (R^2 values), effect size, and collinearity statistics. Secondly, using a bootstrapping approach to test the structural model relationships significance. In such approach, the collected data sample is treated as the population sample where the algorithm used a replacement technique to generate a random and large number of bootstrap samples (recommended to predefine as 5000) all with the same amount of cases as the original sample (Henseler et al. 2009). The present study conducted the bootstrapping procedure with 5000 bootstrap samples, two-tailed testing, and an assumption of 5% significant level.

Finally, a blindfolding procedure was also used to evaluate the predictive relevance (Q^2) of the structural model. In this approach, part of the data points are omitted and considered missing from the constructs' indicators, and the parameters are estimated using the remaining data points (Hair et al. 2017). These estimations are then used to predict the missing data points which will be compared later with the real omitted data to measure Q^2 value. Blindfolding is considered a sample reuse approach which only applied to endogenous constructs (Henseler et al. 2009). Endogenous constructs are the variables that are affected by other variables in the study model (Götz et al. 2010), such as user susceptibility, involvement, and trust.

Results

The part of the conceptual model that includes the relations between the measurement items and their associated factors is called the measurement model, while the hypothesised relationships among the different factors is called the structural model (Tabachnick and Fidel 2013). The present study's measurement model, which includes all the constructs along with their indicators' outer loadings, can be found in Appendix 3. The result of the measurement model analysis in Table 2 reveals that the

Table 2 Reliability and convergent validity tests

Constructs	Dimensions	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Involvement		0.706	0.733	0.870	0.771
Num_Con		1.000	1.000	1.000	1.000
knownFR		1.000	1.000	1.000	1.000
SNEXP		1.000	1.000	1.000	1.000
Risk	Severity	0.868	0.868	0.919	0.792
	Likelihood	0.829	0.834	0.898	0.746
Competence	Security	0.715	0.715	0.875	0.778
	Privacy	0.710	0.710	0.873	0.775
	Self-efficacy	0.762	0.763	0.894	0.808
CCEXP		0.777	0.923	0.843	0.576
Trust	TrustM	0.867	0.868	0.919	0.791
	TrustP	0.862	0.862	0.916	0.784
Motivation	Hedonic	0.727	0.738	0.879	0.784
	Social	0.709	0.712	0.873	0.774
Susceptibility		0.877	0.896	0.905	0.616

Cronbach alpha and the composite reliability were acceptable for all constructs as they were above the threshold of 0.70. Additionally, since the average variance extracted (AVE) for all constructs was above the threshold of 0.5 (Hair et al. 2017), the convergent validity of the model's reflective constructs was confirmed.

However, in order to assess the model's predictive ability and to examine the significance of relationships between the model's constructs, the structural model should be tested. The assessment of the structural model involves the following testing steps.

Assessing collinearity

This step is vital to determine if there are any collinearity issues among the predictors of each endogenous construct. Failing to do so could lead to a biased path coefficient estimation if a critical collinearity issue exists among the construct predictors (Hair et al. 2017). Table 3 presents all the endogenous constructs (represented by the columns) which indicate that the variance inflation factor (VIF) values for all predictors of each endogenous construct (represented by the rows) are below the threshold of 5. Thus, no collinearity issues exist in the structural model.

Assessing path coefficients (hypotheses testing)

The path coefficient was calculated using the bootstrap re-sampling procedure (Hair et al. 2017). This procedure provides estimates of the direct impact that each construct has on user susceptibility to cyber-attack. The result of the direct effect test in Table 4 shows that trust (t = 5.202, $p < 0.01$) is the highest variable that predicts the user's susceptibility to SE victimisation, followed by user's involvement (t = 5.002, $p < 0.01$), cybercrime experience (t = 3.736, $p < 0.01$), social network experience (t = – 3.015, $p < 0.01$), and percentage of known friends among Facebook connections (t = – 2.735, $p < 0.01$). The direct effects of user competence to deal with threats (t = – 2.474, $p < 0.05$) and the number of connections (t = – 2.428, $p < 0.05$)

Table 3 Collinearity assessment (VIF)

	CCEXP	Competence	Involvement	KnownFR	Risk	Susceptibility	Trust
CCEXP					1.000	1.125	
Competence						1.115	
Involvement	1.034					1.170	1.034
KnownFR						1.112	
Motivation	1.034		1.006			1.152	1.034
Num-Con			1.006			1.075	
Risk		1.000				1.077	
SNEXP				1.000		1.162	
Trust						1.255	

Table 4 Path coefficient results (significance testing- group a)

Hypo	Relationship	Std. Beta	STDEV	T-value	*P*-value	95% Confidence interval	
Ha1	Involvement- > Susceptibility	0.222	0.063	5.002	0.000**	0.098	0.344
Ha2	Num-Con - > Susceptibility	−0.100	0.041	2.428	0.015[a]	−0.181	−0.019
Ha3	KnownFR - > Susceptibility	−0.127	0.047	2.735	0.006**	−0.222	−0.037
Ha4	SNEXP - > Susceptibility	−0.163	0.054	3.015	0.003**	−0.268	– 0.053
Ha5	Risk - > Susceptibility	– 0.058	0.051	1.142	0.254	−0.157	0.041
Ha6	Competence - > Susceptibility	−0.125	0.050	2.474	0.013*	−0.224	−0.029
Ha7	CCEXP - > Susceptibility	0.222	0.059	3.736	0.000**	0.105	0.340
Ha8	Trust - > Susceptibility	0.286	0.055	5.202	0.000**	0.177	0.392
Ha9	Motivation - > Susceptibility	0.015	0.043	0.346	0.729	−0.068	0.099

Significant at ** $p < 0.01$, * $p < 0.05$; [a] statistically significant but in the opposite direction to that hypothesised

were relatively small, yet still statistically significant in explaining the target variable. However, the impact of the number of connections on users' susceptibility was negative which opposes hypothesis (Ha2) that claims that this relationship is positive.

Most importantly, the result indicated that perceived risk and motivation have no direct effect on user's vulnerability ($p > 0.05$). This could be caused by the fact that both factors are second-order formative variables, while their first order factors have different direction effects on user's susceptibility. As can be seen from the result of the regression analysis in Table 5, perceived risk is the second order factor of perceived severity of threat which has a significant negative effect on the user's susceptibility and perceived likelihood of threat which has a positive impact on user's susceptibility. Therefore, their joint effect logically will be not significant, because the opposite effects of the two dimensions of perceived risk have cancelled each other. Thus, Ha5 could be considered as partially supported.

The situation with Motivation is similar as it is also a second-order formative factor and its first order factors (hedonic and social) have an opposite effect on users' susceptibility. Table 5 presents the result of the regression analysis of first-order factors for the motivation construct. The result provides evidence that hedonic motivation is negatively related to the user's susceptibility while social motivation is positively associated with user's susceptibility. However, when the two dimensions of motivation were aggregated to create one index to measure the total effect of user's motivation (both direct and indirect), as illustrated in Table 6, the model revealed a significant predictor of users' susceptibility (t = 3.854, $p < 0.01$). Thus, the direct effect of motivation on user susceptibility is statistically rejected, while the total effect of motivation on users' susceptibility is statistically significant and considered one of the strongest predictors in the study model.

Table 5 Regression analysis of perceived risk and motivation dimensions

Factors	Dimensions	Std. Beta	t	Sig.
Perceived Risk	Severity	−.146	−2.446	.015
	Likelihood	.117	1.958	.051
Motivation	Hedonic	−.080	−1.423	.156
	Social	.319	5.680	.000

Dependent Variable: Susceptibility

Evaluating the total effect of a particular construct on user susceptibility is considered useful, especially if the goal of the study is to explore the impact of the relationships between different drivers to predict one latent construct (Hair et al. 2017). The total impact includes both the construct's direct effect and indirect effects through mediating constructs in the model. The total effect analysis in Table 6 revealed that most of the constructs have a significant overall impact on user susceptibility ($p < 0.05$). Although the number of connections has been proven to have a significant negative direct effect on user susceptibility, its total effect when considering all the direct and indirect relationships seems to be very low and not significant (t = – 0.837, $p > 0.05$). Furthermore, both the direct and total effect of perceived risk has been found to be not substantial (t = – 1.559, $p > 0.05$).

The rest of the hypotheses (group b) aim to examine the relationships between the independent constructs of the study model, which will be tested according to estimates of the path coefficient between the related constructs. Table 7 shows that all nine hypotheses are statistically significant ($p < 0.05$). This also shows the most substantial relationship was between social network experience and the percentage of known friends among Facebook connections (t = 6.091, $p < 0.01$), followed by the favourable impact motivation and level of involvement have on increasing users trust (with t-value = 4.821, and t-value = 3.914, respectively).

Table 6 Total effects significance testing results

Hypo	Relationship	Std. Beta	STDEV	T-value	*P*-value	95% Confidence interval		Sig.?
Ha1	Involvement - > Susceptibility	0.320	0.064	5.002	0.000	0.188	0.441	Yes
Ha2	Num-Con - > Susceptibility	−0.037	0.044	0.837	0.403	−0.122	0.050	No
Ha3	KnownFR - > Susceptibility	−0.127	0.047	2.735	0.006	−0.224	−0.041	Yes
Ha4	SNEXP - > Susceptibility	−0.201	0.050	4.028	0.000	−0.302	−0.105	Yes
Ha5	Risk - > Susceptibility	−0.078	0.050	1.559	0.119	−0.176	0.024	No
Ha6	Competence - > Susceptibility	−0.125	0.050	2.474	0.013	−0.218	−0.023	Yes
Ha7	CCEXP - > Susceptibility	0.208	0.059	3.552	0.000	0.090	0.322	Yes
Ha8	Trust - > Susceptibility	0.286	0.055	5.202	0.000	0.180	0.395	Yes
Ha9	Motivation - > Susceptibility	0.173	0.045	3.854	0.000	0.082	0.257	Yes

Furthermore, motivation (t = 3.640, $p < 0.01$) and the number of connections (t = 3.106, $p < 0.01$) are two factors found to increase users' level of involvement in the network. Level of involvement also plays a notable role in raising people's previous experience with cybercrime (t = 2.532, $p < 0.05$), while past cybercrime expertise significantly increases people's perceived risk associated with using Facebook (t = 2.968, $p < 0.01$). Nevertheless, the contribution of perceived risk in raising user competence level to deal with online threats was not very strong, although considered statistically significant (t = 2.241, $p < 0.05$).

Finally, there was no significant difference with regard to the user characteristics that affect people's susceptibility or resistance to the high-risk scenarios and low-risk scenarios. This means that participants rely on their perceptions and experience to judge those scenarios.

The coefficient of determination - R^2

The coefficient of determination is a traditional criterion that is used to evaluate the structural model's predictive power. In this study, this coefficient measure will represent the joint effect of all the model variables in explaining the variance in people's susceptibility to SE attacks. According to Hair et al. (2017), the acceptable R^2 value is hard to determine as it might vary depending on the study discipline and the model complexity. Cohen (1988) has suggested a rule of thumb to assess the R^2 values for models with several independent variables which are: 0.26, 0.13, and 0.02 to be considered substantial, moderate, and weak respectively. Table 8 illustrates the coefficient of determination for the endogenous variables in the study model. The R^2 values indicate that the nine prediction variables together have substantial predictive power and explain 33.5% of the variation in users' susceptibility to SE attacks. Furthermore, users' involvement and motivation combined effect on users' trust is considered moderate as it explains 13.2% of the variation in users' trust.

Predictive relevance Q^2

To measure the model's predictive capabilities, a blindfolding procedure has been used to obtain the model's predictive relevance (Q^2 value). Stone-Geisser's Q^2 value, which is a measure to assess how well a model predicts the data of omitted cases, should be higher than zero in order to indicate that the path model has a cross-validated predictive relevance (Hair et al. 2017). Table 8 presents results of the predictive relevance test and shows that all of the endogenous constructs in the research model have predictive relevance greater than zero, which means that the model has appropriate predictive ability.

Table 7 Path coefficient results (significance testing- group b)

Hypo	Relationship	Std. Beta	STDEV	T-value	*P*-value	95% Confidence interval	
Hb1	Involvement - > CCEXP	0.170	0.067	2.532	0.011*	0.031	0.295
Hb2	Involvement - > Trust	0.219	0.056	3.914	0.000**	0.105	0.327
Hb3	Num-Con - > Involvement	0.197	0.063	3.106	0.002**	0.080	0.324
Hb4	SNEXP - > KnownFR	0.302	0.050	6.091	0.000**	0.201	0.394
Hb5	Risk - > Competence	0.165	0.074	2.241	0.025*	0.020	0.311
Hb6	CCEXP - > Risk	0.179	0.060	2.968	0.003**	0.062	0.294
Hb7	Motivation - > Trust	0.253	0.053	4.821	0.000**	0.150	0.353
Hb8	Motivation - > Involvement	0.166	0.046	3.640	0.000**	0.078	0.256
Hb9	Motivation - > CCEXP	0.154	0.055	2.795	0.005**	0.046	0.264

Significant at ** $p < 0.01$; * $p < 0.05$

Table 8 Coefficient of determination (R^2) and predictive relevance (Q^2)

Construct	R Square	R Square Adjusted	Interpretation	SSO	SSE	Q^2 (=1-SSE/SSO)
Susceptibility	0.335	0.315	substantial	316.00	222.74	0.295
Involvement	0.072	0.066	weak	316.00	297.18	0.060
KnownFR	0.091	0.088	weak	316.00	288.18	0.088
Risk	0.032	0.029	weak	316.00	306.36	0.031
Competence	0.027	0.024	weak	316.00	309.17	0.022
CCEXP	0.062	0.056	weak	316.00	300.16	0.050
Trust	0.132	0.127	Moderate	316.00	277.69	0.121

Model fit

Hair et al. (2017) and Henseler et al. (2014) have recommended using SRMR and RMS_{theta} as indices to test a model's goodness of fit. While, SRMR represents the discrepancy between the observed correlations and the model's implied correlations where its cut-point value should be less than 0.08 (Hu and Bentler 1998), RMS_{theta} value of less than 0.12 represents an appropriate model fit (Hair et al. 2017; Henseler et al. 2014). Normed Fit Index (NFI) is an incremental model fit evaluation approach which compares the structural model with a null model of entirely uncorrelated variables, whereby an NFI value of more than 0.90 represents good model fit (Bentler and Bonett 1980). Additionally, Dijkstra and Henseler (2015), recommend using the squared euclidean distance (d_{LS}) and the geodesic distance (d_G) as measures to assess model fit by comparing the distance between the sample covariance matrix and a structured covariance matrix. Comparing the original values of d_{LS} and d_G with their confidence intervals could indicate a good model fit if their values are less than the upper bound of the 95% confidence interval.

Table 9 illustrates the result of the model fit indices that was obtained from the SmartPLS report. The empirical test of the structural model revealed a good model fit as the SRMR value was 0.05, the RMS_{theta} value was 0.099, the NFI was 0.858, which, if rounded, will be 0.9, and the values of d_{LS} and d_G were less than the upper bound of their confidence interval. Thereby, the results of all the considered model fit indices reflect a satisfactory model fit when considering the complexity of the present study model.

Table 9 Model fit criterion

	Estimated Model	95% Confidence interval	
SRMR	0.053	–	–
rms Theta	0.099	–	–
NFI	0.858	–	–
d_{LS}	0.154	0.041	0.155
d_G	0.030	0.009	0.031

Demographic variables effect

One of the present study goals is to examine if specific users' demographics (age, gender, education, and major) are associated with users' susceptibility to social engineering attacks. To explore this relationship, regression analysis, as well as variance tests such as t-test and ANOVA test, have been conducted. Table 10 summarises these tests results.

Gender has been found to affect the user's susceptibility to SE victimisation (Std. beta = 0.133, $p < 0.05$) and the t-test indicates that women are more vulnerable to victimisation (t(271.95) = 2.415, $p < 0.05$). Also, the user's major has a significant effect on the user's vulnerability (Std. beta = 0.112, $p < 0.05$). When comparing the groups' behaviour via ANOVA test, users who are specialised in technical majors such as computer and engineering have been indicated as less susceptible to social engineering attacks than those specialised in humanities and business (F(6) = 5.164, $p < 0.001$). Furthermore, the results show that age has no significant impact on user vulnerability (Std. beta = 0.096, $p > 0.05$). However, when comparing the means of age groups, it can be seen that younger adults (M = 1.97, SD = 0.99) are less susceptible than older adults (M = 2.56, SD = 0.92). Moreover, the educational level has no significant impact on users' vulnerability as revealed by the result of the regression analysis (Std. beta = 0.068, $p > 0.05$).

Discussion

Facebook users' involvement level is revealed in the present study to have a strong significant effect on their susceptibility to SE victimisation. This finding confirms the results of previous research (Saridakis et al. 2016; Vishwanath 2015). Since most social network users are highly involved in online networks, it is hard to generalise that all involved people are vulnerable. However, high involvement affects other critical factors in the present model, i.e., experience with cybercrime and trust, which in turn have powerful impacts on users' susceptibility to victimisation.

The number of friends has been found to have a direct negative impact on people's vulnerability, which is against what the present study hypothesised, as this relationship

Table 10 Demographic factors impact on user susceptibility to SE

Demographic Variable	Regression Analysis			Variance Test		Means						
	Std. Beta	t	Sig.	t-value/ f-value	Sig.							
Gender	0.133	2.381	0.018	−2.415	0.016	Male			Female			
						1.87			2.14			
Age	0.096	1.714	0.088	1.932	0.124	18–24	25–34		35–44		45–55	
						1.97	2.28		1.95		2.56	
Education	0.068	1.201	0.231	0.919	0.432	High school	Bachelor		Master		Other	
						1.98	2.12		1.93		2.7	
Major	0.112	1.990	0.047	5.164	< 0.001	Comp/IT	Eng	Bus	Med	Sci	Hum	Other
						1.78	1.89	2.72	2.46	2.23	2.57	2.05

had been assumed to be positive in order to concur with previous claims that large network size makes individuals more vulnerable to SNs risks (Buglass et al. 2016; Vishwanath 2015). Facebook users seem to accept friend requests from strangers to expand their friendship network. Around 48% of the participants in this study stated that they know less than 10% of their Facebook network personally. Connecting with strangers on the network has previously been seen as the first step in falling prey to social engineering attacks (Vishwanath 2015), while also being regarded as a measure of risky behaviour on social networks (Alqarni et al. 2016). A high percentage of strangers with whom the user is connected can be seen as a determinant of the user's low level of suspicion.

Furthermore, social network experience has been found to significantly predict people's susceptibility to social engineering in the present study. People's ability to detect social network deception has been said to depend on information communication technology literacy (Tsikerdekis and Zeadally 2014). Thus, experienced users are more familiar with cyber-attacks such as phishing and clickjacking, and easily detect them. This is further supported by Algarni et al. (2017), who pointed out that the less time that has elapsed since the user joined Facebook, the more susceptible he or she is to social engineering. Yet, their research treated user experience with social networks as a demographic variable and did not examine whether this factor might affect other aspects of user behaviour. For instance, results from the present study reveal that users who are considered more experienced in social networks have fewer connections with strangers (t = 6.091, $p < 0.01$), which further explains why they are less susceptible than novice users.

Perception of risk has no direct influence on people's vulnerability, but the present study found perceived risk to significantly increase people's level of competence to deal with social engineering attacks. This also accords with the Van Schaik et al. (2018) study, which found that Facebook users with high risk perception adopt precautionary behaviours such as restrictive privacy and security-related settings. Most importantly, perceived cybercrime risk has also been indicated as influencing people to take precautions and avoid using online social networks (Riek et al. 2016).

Measuring user competence levels would contribute to our understanding of the reasons behind user weakness in detecting online security or privacy threats. In the present study, the measure of an individual's competence level in dealing with cybercrime was based upon three dimensions: security awareness, privacy awareness, and self-efficacy. The empirical results show that this competence measure can significantly predict the individual's ability to detect SE attacks on Facebook. Individuals' perception of their self-ability to control the content shared on social network websites has been previously considered a predictor of their ability to detect social network threats (Saridakis et al. 2016), as individuals who have this confidence in their self-ability as well as in their security knowledge seem to be competent in dealing with cyber threats (Flores et al. 2015; Wright and Marett 2010).

Furthermore, our results accord with the finding of Riek et al. (2016) that previous cybercrime experience has a positive and substantial impact on users' perceived risk. Yet, this high-risk perception did not decrease users' vulnerability in the present study. This could be because experience and knowledge of the existence of threats do not need to be reflected in people's behaviour. For example, individuals who had previously undertaken security awareness training still underestimated the importance of some security practices, such as frequent change of passwords (Kim 2013).

The present research found that people's trust in the social network's provider and members were the strongest determinants of their vulnerability to social engineering attacks (t = 5.202, $p < 0.01$). Previous email phishing research (e.g., Alseadoon et al. 2015; Workman 2008) has also stressed that people's disposition to trust has a significant impact on their weakness in detecting phishing emails. Yet, little was known about the impact of trust in providers and other members of social networks on people's vulnerability to cyber-attacks. These two types of trust have been found to decrease users' perception of the risks associated with disclosing private information on SNs (Cheung et al. 2015). Similarly, trusting social network providers to protect members' private information has caused Facebook users (especially females) to be more willing to share their photos in the network (Beldad and Hegner 2017). These findings draw attention to the huge responsibility that social network providers have to protect their users. In parallel, users should be encouraged to be cautious about their privacy and security.

People's motivation to use social networks has no direct influence on their vulnerability to SE victimisation, as evidenced by the results of this study. Yet, this motivation significantly affects different essential aspects of user behaviour and perception such as user involvement, trust, and previous experience with cybercrime, which in turn substantially predict user vulnerability. This result accords with the claim that people's motivation of using SNs increase their disclosure of private information (Beldad and Hegner 2017; Chang and Heo 2014).

Theoretical and practical implications

Most of the proposed measures to mitigate SE threats in the literature (e.g. (Fu et al. 2018; Gupta et al. 2018)) are focused on technical solutions. Despite the importance and effectiveness of these proposed technical solutions, social engineers try to exploit human vulnerabilities; hence we require solutions that understand and guard against human weaknesses. Given the limited number of studies that investigate the impact of human characteristics on predicting vulnerability to social network security threats, the present study can be considered useful, having critical practical implications that should be acknowledged in this section.

The developed conceptual model shows an acceptable prediction ability of people's vulnerability to social engineering in social networks as revealed by the results of this study. The proposed model could be used by information security researchers (or researchers from different fields) to predict responses to different security-oriented risks. For instance, decision-making research could benefit from the proposed framework and model as they indicate new perspectives on user-related characteristics that could affect decision-making abilities in times of risk.

Protecting users' personal information is an essential element in promoting sustainable use of social networks (Kayes and Iamnitchi 2017). SN providers should provide better privacy rules and policies and develop more effective security and privacy settings. A live chat threat report must be essential in SN channels in order to reduce the number of potential victims of specific threatening posts or accounts. Providing security and privacy-related tools could also help increase users' satisfaction with social networks.

Despite the importance of online awareness campaigns as well as the rich training programs that organisations adopt, problems persist because humans are still the weakest link (Aldawood and Skinner 2018). Changing beliefs and behaviour is a complex procedure that needs more research. However, the present study offers clear insight into specific individual characteristics that make people more vulnerable to cybercrimes. Using these characteristics to design training programs is a sensible approach to the tuning of security awareness messages. Similarly, our results will be helpful in conducting more successful training programs that incorporate the identified essential attributes from the proposed perspectives, as educational elements to increase people's awareness. While these identified factors might reflect a user's weak points, the factors could also be targeted by enforcing behavioural security strategies in order to mitigate social engineering threats.

The developed conceptual model could be used in the assessment process for an organisation's employees, especially those working in sensitive positions. Also, the model and associated scales could be of help in employment evaluation tests, particularly in security-critical institutions, since the proposed model may predict those weak aspects of an individual that could increase his/her vulnerability to social engineering.

A semi-automated security advisory system

One of the practical usefulness of the proposed prediction model can be demonstrated through integrating this model in a semi-automated advisory system (Fig. 2). Based on the idea of user profiling, this research has established a practical solution which can semi-automatically predict users' vulnerability to various types of social engineering attacks.

The designed semi-automated advisory system could be used as an approach with which to classify social network users according to their vulnerability type and level after completing an assessment survey. The local administrator can determine the threshold and the priority for each type of attack based on their knowledge. Then, the network provider could send awareness posts to each segment that target the particular group's needs. Assessing social network users and segmenting them based on their behaviour and vulnerabilities is essential in order to design relevant advice that meets users' needs. Yet, since social engineering techniques are rapidly changing and improving, the attack scenarios that are used in the assessment step could be updated from time to time. The registered users in the semi-automated advisory system also need to be reassessed regularly in order to observe any changes in their vulnerability.

Significant outcomes were noted with practical implications for how social network users could be assessed and segmented based on their characteristics, behaviour, and vulnerabilities, in turn facilitating their protection from such threats by targeting them with relevant advice

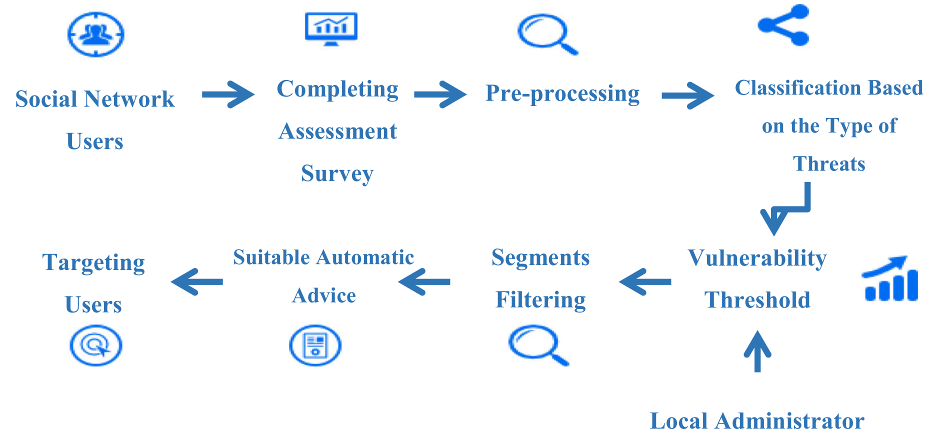

Fig. 2 A Semi-Automated Advisory System

and education that meets users' needs. This system is considered cost and time effective, as integrating individuals' needs with the administrator's knowledge of existing threats could avoid the overhead and inconvenience of sending blanket advice to all users.

Conclusion

The study develops a conceptual model to test the factors that influence social networks users' judgement of social engineering-based attacks in order to identify the weakest points of users' detection behaviour, which also helps to predict vulnerable individuals. Proposing such a novel conceptual model helped in bridging the gap between theory and practice by providing a better understanding of how to predict vulnerable users. The findings of this research indicate that most of the considered user characteristics influence users' vulnerability either directly or indirectly. This research also contributes to the existing knowledge of social engineering in social networks, particularly augmenting the research area of predicting user behaviour toward security threats by proposing a new influencing perspective, the socio-emotional, which has not been satisfactorily reported in the literature before, as a dimension affecting user vulnerability. This new perspective could also be incorporated to investigate user behaviour in several other contexts.

Using a scenario-based experiment instead of conducting a real attack study is one of the main limitations of the present study but was considered unavoidable due to ethical considerations. However, the selected attack scenarios were designed carefully to match recent and real social engineering-based attacks on Facebook. Additionally, the present study was undertaken in full consciousness of the fact that when measuring people's previous experience with cybercrime, some participants might be unaware of their previous victimisation and so might respond inaccurately. In order to mitigate this limitation, different types of SE attacks have been considered in the scale that measures previous experience with cybercrime, such as phishing, identity theft, harassment, and fraud.

Furthermore, this research has focused only on academic communities as all the participants in this study were students, academic, and administrative staff of two universities. This could be seen as a limitation as the result may not reflect the behaviour of the general public. The university context is important however, and cybercriminals have targeted universities recently due to their importance in providing online resources to their students and community (Öğütçü et al. 2016). Additionally, while several steps have been taken to ensure the inclusion of all influential factors in the model, it is not feasible to guarantee that all possibly influencing attributes are included in this study. Further efforts are needed in this sphere, as predicting human behaviour is a complex task.

The conceptual study model could be used to test user vulnerability to different types of privacy or security hazards associated with the use of social networks: for instance, by measuring users' response to the risk related to loose privacy restrictions, or to sharing private information on the network. Furthermore, investigating whether social networks users have different levels of vulnerability to privacy and security associated risks is another area of potential future research. The proposed model's prediction efficiency could be compared to different types of security and privacy threats. This comparison would offer a reasonable future direction for researchers to consider. Future research could focus more on improving the proposed model by giving perceived trust greater attention, as this factor was the highest behaviour predictor in the present model. The novel conceptualisation of users' competence in the conceptual model has proved to have a profound influence on their behaviour toward social engineering victimisation, a finding which can offer additional new insight for future investigations.

Appendix 1

Table 11 Measurement items

Construct	Dimensions	Questions	Measurement items
Perceived Risk	Severity of threat	• Please choose the best answer in each statement that indicates the extent to which a statement is true for you: (from Strongly agree to Strongly disagree)	• I believe that losing my data privacy while using Facebook would be a severe problem for me (ST2) • I believe that having my messages and chats being seen or listened to in Facebook would be a severe problem for me (ST3) • I believe that losing my financial information while using Facebook would be harmful for me (ST4)
	Likelihood of threat	• Answer the following questions according to your beliefs, attitudes, and experiences: (from Extremely Likely to Extremely Unlikely)	• How likely is it for your financial information to be stolen in Facebook? (LT1) • How likely is it that your identity can be stolen in Facebook? (LT2) • How likely is it for your privacy to be invaded without your knowledge while using Facebook? (LT3)
Competence	Security	• Please choose the best answer in each statement that indicates the extent to which a statement is true for you: (from Strongly agree to Strongly disagree)	• I use password for my Facebook account different from the passwords I use to access other sites (SA2) • I use a specific new email for my Facebook account different from my personal or work email (SA4)
	Privacy	• Please choose the best answer in each statement that indicates the extent to which a statement is true for you: (from Strongly agree to Strongly disagree)	• I don't share personal information on Facebook such as birthdate, phone number, workplace or address (PA3) • I don't share my current or future location on Facebook for example, images for my current vacation, or plans for future vacation (PA4)
	Self-efficacy	• Please choose the best answer in each statement that indicates the extent to which a statement is true for you: (from Strongly agree to Strongly disagree)	• I have the knowledge and the ability to secure my Facebook account by adjusting the account settings (SEF3) • I have the ability to protect myself from any online threats while using Facebook (SEF4)
Past experience with cybercrime		• How often have you experienced or been a victim of the following incidents? (Rate each statement from always to never)	• Identity theft (somebody stealing your personal data and impersonating you, e.g. Open SN account with your name, or Shopping under your name) (PE1_It) • Phishing (Received emails fraudulently asking for money or personal details, including banking or payment information) (PE2_Ph) • Online fraud where goods purchased were not delivered, counterfeit or not as advertised (PE3_OF) • Harassment, cyber-bullying (Received Harassing messages, inappropriate comments, or other persistent behaviours that endangers your safety) (PE4_Har)
Trust	Trust Provider	• Please choose the best answer that indicates how much you agree with the following statements: (from Strongly agree to Strongly disagree)	• Facebook is a trustworthy social network (TP1) • I can count on Facebook to protect my privacy (TP2) • I can count on Facebook to protect my personal information from unauthorized use (TP3)
	Trust Members	• Please choose the best answer that indicates how much you agree with the following statements: (from Strongly agree to Strongly disagree)	• Facebook Members will not take advantage of others even when the opportunity arises (TM1) • Facebook Members are truthful in dealing with one another (TM3) • Facebook Members will always keep the promises they make to one another (TM4)
Motivation	Hedonic	• What are your main reasons of using social networks? (Rate each statement from Strongly agree to Strongly disagree)	• To pass the time (HM1) • Using social networks are enjoyable and entertaining (HM2)
	Social	• What are your main reasons of using social networks? (Rate each statement from Strongly agree to Strongly disagree)	• To keep in touch with friends and family (SM1) • To maintain my popularity and prestige among peers (SM3)

Appendix 2

Table 12 A Summary of the social engineering scenarios

Type of Trick	Message	Risk-level
1. Phishing – requesting sensitive information such as the user's email and real name in order to win an iPhone 7 or £100 voucher.	Winner picked tonight Like = free iphone7 Comment = £100 voucher To contact you if you win, Enter your email and name here http://bit.ly/2gno8tj	High
2. Clickjacking with an executable file- a post about a shocking and a very important document that is shown in the post as a pdf file with the mouse pointer positioned on the link and the actual URL in the status bar indicates that the document is an executable file.	I don't want to believe. I just read this document. You must read it. it is very important for all public. Please someone tell me that is a lie.	High
3. Clickjacking- a post that includes a video that direct the user to an ambiguous link. However, this type of link is a low-risk since the link could be either a malicious link or a safe link; it is not clear and not safe to risk and clicks in such links.	Video: The most shocking viedo you will every watch!!	Low
4. Malware- offering an application that allows users to call and message their friends free of charge if they ignore the warning message and give permission to the application to access their profile and contact information.	Download this app. It's works perfect for calling out or messaging. All you need is Wi-Fi.	High
5. Phishing scam- a threatening message pretended to be from Facebook support team asking the user to re-confirm his/her account or blocking the account. The link in the message is the original Facebook site, but the actual URL displayed in the status bar is http://cut.uk/Facebookconfirm-login, which is apparently a phishing site.	Your account is at risk! Please re-confirm your account to avoid plocking, if you are the original owner of this account. Please re-confirm you account by following this link here: https://www.facebook.com/xsrn if you don't confirm our system will automatically block your account and will not be able to use it again.	High
6. Click on a safe link- YouTube video that shows recent news, the link appears in the bottom status bar shows a YouTube short link. Such short URLs could be either malicious links or safe links.	OMG..Tsunami hitting again ☹	Low

Appendix 3

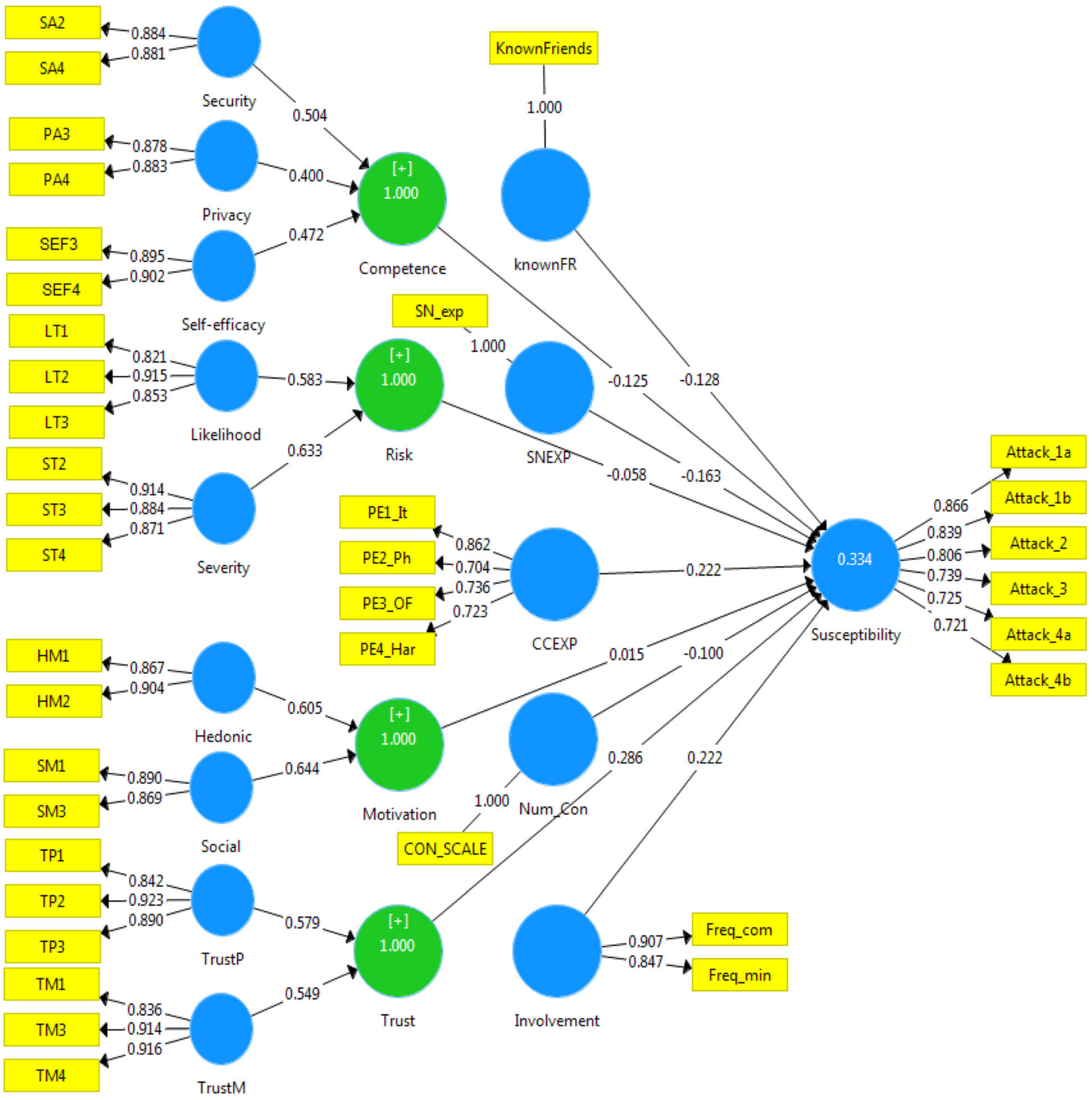

Fig. 3 Measurement Model

Acknowledgements
We are sincerely grateful to the many individuals who voluntarily participated in this research.

Authors' contributions
SMA conducted the study, analysed the collected data, and drafted the manuscript. GRSW participated in drafting the manuscript. Both authors read and approved the final manuscript.

Funding
This work is supported by the University of Jeddah, Kingdom of Saudi Arabia as part of the first author's research conducted at the University of Strathclyde in Glasgow, UK.

Availability of data and materials
The data that support the findings of this study are available from the corresponding author upon reasonable request.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]College of Computer Science and Engineering, University of Jeddah, Jeddah, Kingdom of Saudi Arabia. [2]Department of Computer and Information Sciences, University of Strathclyde, Glasgow, UK.

Received: 8 October 2019 Accepted: 20 February 2020
Published online: 05 March 2020

References

Al Omoush KS, Yaseen SG, Atwah Alma'Aitah M (2012) The impact of Arab cultural values on online social networking: the case of Facebook. Comput Hum Behav 28(6):2387–2399. https://doi.org/10.1016/j.chb.2012.07.010

Albladi SM, Weir GRS (2017) Competence measure in social networks. In: 2017 International Carnahan Conference on Security Technology (ICCST). IEEE, pp 1–6. https://doi.org/10.1109/CCST.2017.8167845

Albladi SM, Weir GRS (2018) User characteristics that influence judgment of social engineering attacks in social networks. Hum-Cent Comput Info Sci 8(1):5. https://doi.org/10.1186/s13673-018-0128-7

Aldawood H, Skinner G (2018) Educating and raising awareness on cyber security social engineering: a literature review. In: 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering. IEEE, pp 62–68. https://doi.org/10.1109/TALE.2018.8615162

Algarni A, Xu Y, Chan T (2017) An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. Eur J Inf Syst 26(6):661–687. https://doi.org/10.1057/s41303-017-0057-y

Alqarni Z, Algarni A, Xu Y (2016) Toward predicting susceptibility to phishing victimization on Facebook. In: 2016 IEEE International Conference on Services Computing (SCC). IEEE, pp 419–426. https://doi.org/10.1109/SCC.2016.61

Alseadoon IMA (2014) The impact of users' characteristics on their ability to detect phishing emails. Doctoral Thesis. Queensland University of Technology. https://eprints.qut.edu.au/72873/.

Alseadoon I, Othman MFI, Chan T (2015) What is the influence of users' characteristics on their ability to detect phishing emails? In: Sulaiman HA, Othman MA, Othman MFI, Rahim YA, Pee NC (eds) Advanced computer and communication engineering technology, vol 315. Springer International Publishing, Cham, pp 949–962. https://doi.org/10.1007/978-3-319-07674-4_89

Baabdullah AM (2018) Consumer adoption of Mobile Social Network Games (M-SNGs) in Saudi Arabia: the role of social influence, hedonic motivation and trust. Technol Soc 53:91–102. https://doi.org/10.1016/j.techsoc.2018.01.004

Basak E, Calisir F (2015) An empirical study on factors affecting continuance intention of using Facebook. Comput Hum Behav 48:181–189. https://doi.org/10.1016/j.chb.2015.01.055

Beldad AD, Hegner SM (2017) More photos from me to thee: factors influencing the intention to continue sharing personal photos on an Online Social Networking (OSN) site among young adults in the Netherlands. Int J Hum–Comput Interact 33(5):410–422. https://doi.org/10.1080/10447318.2016.1254890

Bentler PM, Bonett DG (1980) Significance tests and goodness of fit in the analysis of covariance structures. Psychol Bull 88(3):588–606. https://doi.org/10.1037//0033-2909.88.3.588

Bohme R, Moore T (2012) How do consumers react to cybercrime? In: 2012 eCrime Researchers Summit. IEEE, pp 1–12. https://doi.org/10.1109/eCrime.2012.6489519

Buglass SL, Binder JF, Betts LR, Underwood JDM (2016) When 'friends' collide: social heterogeneity and user vulnerability on social network sites. Comput Hum Behav 54:62–72. https://doi.org/10.1016/j.chb.2015.07.039

Cao B, Lin W-Y (2015) How do victims react to cyberbullying on social networking sites? The influence of previous cyberbullying victimization experiences. Comput Hum Behav 52:458–465. https://doi.org/10.1016/j.chb.2015.06.009

Chang C-W, Heo J (2014) Visiting theories that predict college students' self-disclosure on Facebook. Comput Hum Behav 30:79–86. https://doi.org/10.1016/j.chb.2013.07.059

Cheung C, Lee ZWY, Chan TKH (2015) Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence. Internet Res 25(2):279–299. https://doi.org/10.1108/IntR-09-2013-0192

Chiu C-M, Hsu M-H, Wang ETG (2006) Understanding knowledge sharing in virtual communities: an integration of social capital and social cognitive theories. Decis Support Syst 42(3):1872–1888. https://doi.org/10.1016/j.dss.2006.04.001

Chiu C-M, Wang ETG, Fang Y-H, Huang H-Y (2014) Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk. Inf Syst J 24(1):85–114. https://doi.org/10.1111/j.1365-2575.2012.00407.x

Cohen J (1988) Statistical power analysis for the behavioral sciences, 2nd edn

Dijkstra TK, Henseler J (2015) Consistent and asymptotically normal PLS estimators for linear structural equations. Comput Stat Data Anal 81:10–23. https://doi.org/10.1016/j.csda.2014.07.008

Flores WR, Holm H, Nohlberg M, Ekstedt M (2015) Investigating personal determinants of phishing and the effect of national culture. Inf Comput Secur 23(2):178–199. https://doi.org/10.1108/ICS-05-2014-0029

Flores WR, Holm H, Svensson G, Ericsson G (2014) Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Inf Manag Comput Secur 22(4):393–406. https://doi.org/10.1108/IMCS-11-2013-0083

Fogel J, Nehmad E (2009) Internet social network communities: risk taking, trust, and privacy concerns. Comput Hum Behav 25(1):153–160. https://doi.org/10.1016/j.chb.2008.08.006

Fu Q, Feng B, Guo D, Li Q (2018) Combating the evolving spammers in online social networks. Comput Secur 72:60–73. https://doi.org/10.1016/j.cose.2017.08.014

Gao H, Hu J, Huang T, Wang J, Chen Y (2011) Security issues in online social networks. IEEE Internet Comput 15(4):56–63. https://doi.org/10.1109/MIC.2011.50

Götz O, Liehr-Gobbers K, Krafft M (2010) Evaluation of structural equation models using the partial least squares (PLS) approach. In: Esposito Vinzi V, Chin W, Henseler J, Wang H (eds) Handbook of partial least squares. Springer Berlin Heidelberg, pp 691–711. https://doi.org/10.1007/978-3-540-32827-8_30

Gupta BB, Arachchilage NAG, Psannis KE (2018) Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun Syst 67(2):247–267. https://doi.org/10.1007/s11235-017-0334-z

Hair JF, Hult GTM, Ringle CM, Sarstedt M (2017) A primer on partial least squares structural equation modeling (PLS-SEM), 2nd edn. SAGE Publications. https://search.lib.byu.edu/byu/record/lee.6690785.

Hair JF, Sarstedt M, Ringle CM, Mena JA (2012) An assessment of the use of partial least squares structural equation modeling in marketing research. J Acad Mark Sci 40(3):414–433. https://doi.org/10.1007/s11747-011-0261-6

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and Facebook. ArXiv Preprint. Retrieved from http://arxiv.org/abs/1301.7643

Henseler J, Dijkstra TK, Sarstedt M, Ringle CM, Diamantopoulos A, Straub DW et al (2014) Common beliefs and reality about PLS. Organ Res Methods 17(2):182–209. https://doi.org/10.1177/1094428114526928

Henseler J, Ringle CM, Sinkovics RR (2009) The use of partial least squares path modeling in international marketing. Adv Int Mark 20(1):277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Hu L, Bentler PM (1998) Fit indices in covariance structure modeling: sensitivity to underparameterized model misspecification. Psychol Methods 3(4):424–453. https://doi.org/10.1037/1082-989X.3.4.424

Iuga C, Nurse JRC, Erola A (2016) Baiting the hook: factors impacting susceptibility to phishing attacks. Hum-Cent Comput Info Sci 6(1):8. https://doi.org/10.1186/s13673-016-0065-2

Joinson AN (2008) Looking at, looking up or keeping up with people? Motives and uses of Facebook. In: Proceeding of the twenty-sixth annual CHI conference on human factors in computing systems. ACM Press, New York, pp 1027–1036. https://doi.org/10.1145/1357054.1357213

Kayes I, Iamnitchi A (2017) Privacy and security in online social networks: a survey. Online Soc Netw Media 3–4:1–21. https://doi.org/10.1016/j.osnem.2017.09.001

Kim EB (2013) Information security awareness status of business college: undergraduate students. Inf Secur J 22(4):171–179. https://doi.org/10.1080/19393555.2013.828803

Kim YH, Kim DJ, Wachter K (2013) A study of mobile user engagement (MoEN): engagement motivations, perceived value, satisfaction, and continued engagement intention. Decis Support Syst 56(1):361–370. https://doi.org/10.1016/j.dss.2013.07.002

Krombholz K, Hobel H, Huber M, Weippl E (2015) Advanced social engineering attacks. J Inf Secur Appl 22:113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Madden M, Lenhart A, Cortesi S, Gasser U, Duggan M, Smith A, Beaton M (2013) Teens, social media, and privacy. Pew Research Center Retrieved from http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

Mahuteau S, Zhu R (2016) Crime victimisation and subjective well-being: panel evidence from Australia. Health Econ 25(11):1448–1463. https://doi.org/10.1002/hec.3230

Milne GR, Labrecque LI, Cromer C (2009) Toward an understanding of the online consumer's risky behavior and protection practices. J Consum Aff 43(3):449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Mitnick KD, Simon WL (2003) The art of deception: controlling the human element in security. Wiley. https://books.google.com.sa/books?hl=ar&lr=&id=rmvDDwAAQBAJ&oi=fnd&pg=PR7&dq=Mitnick+KD,+Simon+WL+(2003)+The+art+of+deception:+controlling+the+human+1217+element+in+security.+Wiley&ots=_eyXWB11Wd&sig=9QEMsNUp8X2oiGmAnh7S800L160&redir_esc=y#v=onepage&q&f=false.

Munro MC, Huff SL, Marcolin BL, Compeau DR (1997) Understanding and measuring user competence. Inf Manag 33(1):45–57. https://doi.org/10.1016/S0378-7206(97)00035-9

Öğütçü G, Testik ÖM, Chouseinoglou O (2016) Analysis of personal information security behavior and awareness. Comput Secur 56:83–93. https://doi.org/10.1016/j.cose.2015.10.002

Orchard LJ, Fullwood C, Galbraith N, Morris N (2014) Individual differences as predictors of social networking. J Comput-Mediat Commun 19(3):388–402. https://doi.org/10.1111/jcc4.12068

Proofpoint. (2018). The human factor 2018 report. Retrieved from https://www.proofpoint.com/sites/default/files/pfpt-us-wp-human-factor-report-2018-180425.pdf

Rae JR, Lonborg SD (2015) Do motivations for using Facebook moderate the association between Facebook use and psychological well-being? Front Psychol 6:771. https://doi.org/10.3389/fpsyg.2015.00771

Riek M, Bohme R, Moore T (2016) Measuring the influence of perceived cybercrime risk on online service avoidance. IEEE Trans Dependable Secure Comput 13(2):261–273. https://doi.org/10.1109/TDSC.2015.2410795

Ringle CM, Sarstedt M, Straub D (2012) A critical look at the use of PLS-SEM in MIS quarterly. MIS Q 36(1) Retrieved from https://ssrn.com/abstract=2176426

Ringle CM, Wende S, Becker J-M (2015) SmartPLS 3. SmartPLS, Bönningstedt Retrieved from http://www.smartpls.com

Ross C, Orr ES, Sisic M, Arseneault JM, Simmering MG, Orr RR (2009) Personality and motivations associated with Facebook use. Comput Hum Behav 25(2):578–586. https://doi.org/10.1016/j.chb.2008.12.024

Rungtusanatham M, Wallin C, Eckerd S (2011) The vignette in a scenario-based role-playing experiment. J Supply Chain Manag 47(3):9–16. https://doi.org/10.1111/j.1745-493X.2011.03232.x

Saridakis G, Benson V, Ezingeard J-N, Tennakoon H (2016) Individual information security, user behaviour and cyber victimisation: an empirical study of social networking users. Technol Forecast Soc Chang 102:320–330. https://doi.org/10.1016/j.techfore.2015.08.012

Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J (2010) Who falls for phish? In: Proceedings of the 28th international conference on human factors in computing systems - CHI '10. ACM Press, New York, pp 373–382. https://doi.org/10.1145/1753326.1753383

Sherchan W, Nepal S, Paris C (2013) A survey of trust in social networks. ACM Comput Surv 45(4):1–33. https://doi.org/10.1145/2501654.2501661

Soper, D. (2012). A-priori sample size calculator. Retrieved from https://www.danielsoper.com/statcalc/calculator.aspx?id=1

Tabachnick BG, Fidel LS (2013) Using multivariate statistics, 6th edn. Pearson, Boston

Tsikerdekis M, Zeadally S (2014) Online deception in social media. Commun ACM 57(9):72–80. https://doi.org/10.1145/2629612

Van Schaik P, Jansen J, Onibokun J, Camp J, Kusev P (2018) Security and privacy in online social networking: risk perceptions and precautionary behaviour. Comput Hum Behav 78:283–297. https://doi.org/10.1016/j.chb.2017.10.007

Vishwanath A (2015) Habitual Facebook use and its impact on getting deceived on social media. J Comput-Mediat Commun 20(1):83–98. https://doi.org/10.1111/jcc4.12100

Vishwanath A, Harrison B, Ng YJ (2016) Suspicion, cognition, and automaticity model of phishing susceptibility. Commun Res. https://doi.org/10.1177/0093650215627483

Wang J, Herath T, Chen R, Vishwanath A, Rao HR (2012) Research article phishing susceptibility: an investigation into the processing of a targeted spear phishing email. IEEE Trans Prof Commun 55(4):345–362. https://doi.org/10.1109/TPC.2012.2208392

Wang J, Li Y, Rao HR (2017) Coping responses in phishing detection: an investigation of antecedents and consequences. Inf Syst Res 28(2):378–396. https://doi.org/10.1287/isre.2016.0680

Workman M (2007) Gaining access with social engineering: an empirical study of the threat. Inf Syst Secur 16(6):315–331. https://doi.org/10.1080/10658980701788165

Workman M (2008) A test of interventions for security threats from social engineering. Inf Manag Comput Secur 16(5):463–483. https://doi.org/10.1108/09685220810920549

Wright RT, Marett K (2010) The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. J Manag Inf Syst 27(1):273–303. https://doi.org/10.2753/MIS0742-1222270111

Yang H-L, Lin C-L (2014) Why do people stick to Facebook web site? A value theory-based view. Inf Technol People 27(1):21–37. https://doi.org/10.1108/ITP-11-2012-0130

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.